

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-106148

(43)Date of publication of application : 24.04.1998

(51)Int.Cl.

**G11B 20/10**

G06F 12/14

G09C 1/00

H04L 9/08

(21)Application number : 09-136709

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 27.05.1997

(72)Inventor : KATO TAKEHISA

ENDO NAOKI

UNNO HIROAKI

KOJIMA TADASHI

HIRAYAMA KOICHI

(30)Priority

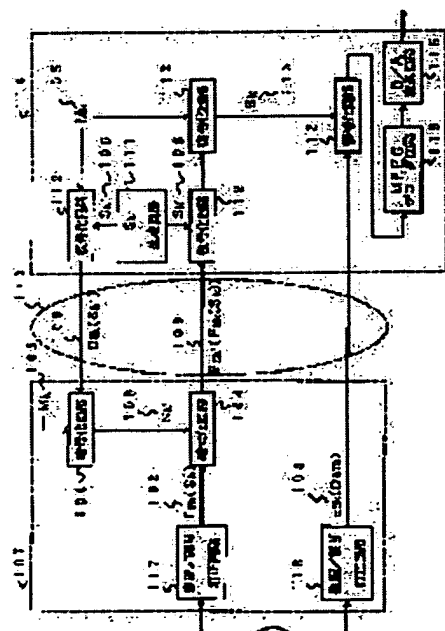
Priority number : 08170399    Priority date : 28.06.1996    Priority country : JP

(54) CIPHERING METHOD, DECODING METHOD, RECORDING AND REPRODUCING  
DEVICE, DECODING DEVICE, DECODING UNIT DEVICE, RECORDING MEDIUM,  
MANUFACTURE OF RECORDING MEDIUM AND METHOD OF MANAGING KEY

(57)Abstract:

**PROBLEM TO BE SOLVED:** To protect a copyright from piracy in preventing illegal copies by ciphering a data with a 1st key and ciphering this 1st key with predetermined plural 2nd keys.

**SOLUTION:** A 2nd session key  $Sk'$  is generated by a session key generating circuit 111, and is decoded by a decoding circuit 112 with a master key  $Mk$  and then ciphered by a ciphering circuit 104 with the key  $Mk$ , so that the key  $Sk'$  generated by the circuit 111 is obtained. Then, a 1st session key ciphered by the key  $Mk$  recorded on a DVD 101 is ciphered by the key  $Sk'$  and is sent to the circuit 112, where this key is decoded by the



key  $M_k$  to obtain the 1st session key  $M_k$ . Then, a data ciphered by a key  $S_k$  recorded on the DVD 101 is read out, and is processed by a demodulation/ error correction circuit 118, and afterward, the received data is decoded by the circuit 112 with the key  $S_k$  to obtain a plain styled data. Thus, the decoded data does not flow in a CPU.BUS 110, and for example, even when this data is stored in a storage medium, the data cannot be reproduced to be used. Consequently, an illegal act of making unauthorized copies is prevented to protect the copyright from piracy.



## 【特許請求の範囲】

【請求項1】第1の鍵でデータを暗号化し、前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化することを特徴とする暗号化方法。

【請求項2】データを第1の鍵で暗号化した情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化した情報とを少なくとも記録したことを特徴とする記録媒体。

【請求項3】データを第1の鍵で暗号化した情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化した情報とを同一の記録媒体内に少なくとも記録することを特徴とする記録媒体の製造方法。

【請求項4】データを第1の鍵で暗号化した情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化した情報とを少なくとも入力し、前記第2の鍵の少なくとも一つを用いて前記第1の鍵を復号して得て、得られた第1の鍵が正しいものであることを所定の方法により判定した後に、この第1の鍵を用いて前記データを復号して得ることを特徴とする復号方法。

【請求項5】データを第1の鍵で暗号化した情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化した情報とを少なくとも入力する入力手段と、前記第2の鍵の少なくとも一つを記憶する記憶手段と、この記憶手段内の前記第2の鍵の少なくとも一つを用いて前記入力手段から入力された情報に基づいて前記第1の鍵を復号して得て、得られた第1の鍵が正しいものであることを所定の方法により判定した後に、この第1の鍵を用いて前記データを復号して得る復号手段とを備えたことを特徴とする復号装置。

【請求項6】データを第1の鍵で暗号化した情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化した情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し手段と、前記第2の鍵の少なくとも一つを記憶する記憶手段と、この記憶手段内の前記第2の鍵の少なくとも一つを用いて前記読み出し手段から読み出された情報に基づいて前記第1の鍵を復号して得て、得られた第1の鍵が正しいものであることを所定の方法により判定した後に、この第1の鍵を用いて前記データを復号して得る復号手段とを備えたことを特徴とする記録再生装置。

【請求項7】第1の管理者に予め定められた複数の第2の鍵を少なくとも保管させ、第2の管理者にデータを第1の鍵で暗号化した情報と前記第1の鍵を前記予め定められた複数の第2の鍵でそれぞれ暗号化した情報とを少なくとも管理させ、第3の管理者に前記第2の鍵の少なくとも一つを管理させることを特徴とする鍵の管理方法。

【請求項8】データを第1の鍵で暗号化して得られた第1の情報と前記第1の鍵を予め定められた複数の第2の

鍵でそれぞれ暗号化して得られた第2の情報と鍵判定に用いる第3の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し手段と、前記第2の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第2の鍵のうちから定められた順番に従い選択した一つ用いて、前記第2の情報のうちから定められた順番に従い選択した一つの暗号化された第1の鍵を復号するとともに、少なくともこの復号結果と前記第3の情報とをもとにして、前記復号により得られたこの第1の鍵が正しいものであるか否かを判定し、正しいものと判定された第1の鍵が得られるまで前記選択および前記判定を繰り返す第1の復号手段と、

この第1の復号手段により正しいものとして得られた前記第1の鍵を用いて前記データを復号して得る第2の復号手段とを備えたことを特徴とする復号装置。

【請求項9】記録媒体から少なくとも読み出された、データを第1の鍵で暗号化して得られた第1の情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化して得られた第2の情報と鍵判定に用いる第3の情報とを、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のCPUバスを介さず接続された第1のユニットから計算機のCPUバスを介して第2のユニットに伝え、前記第2のユニットにおいて少なくとも前記データの復号を行う復号装置であって、

前記第1のユニットは、前記計算機のCPUバスを介して前記第2のユニットへ、前記第1、第2および第3の情報を伝えるときに、少なくとも前記第2および第3の情報については、外部から取得されることなく安全に伝えるための手段を備え、

前記第2のユニットは、前記計算機のCPUバスを介して前記第1のユニットから、前記第1、第2および第3の情報を受け取るときに、少なくとも前記第2および第3の情報については、外部から取得されることなく安全に受け取るための手段と、

前記第2の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第2の鍵のうちから定められた順番に従い選択した一つ用いて、前記第2の情報のうちから定められた順番に従い選択した一つの暗号化された第1の鍵を復号するとともに、少なくともこの復号結果と前記第3の情報とをもとにして、前記復号により得られたこの第1の鍵が正しいものであるか否かを判定し、正しいものと判定された第1の鍵が得られるまで前記選択および前記判定を繰り返す第1の復号手段と、

この第1の復号手段により正しいものとして得られた前記第1の鍵を用いて前記データを復号して得る第2の復号手段とを備えたことを特徴とする復号装置。

【請求項10】第3の鍵を第1の鍵で暗号化して得られ

た第1の情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化して得られた第2の情報と鍵判定に用いる第3の情報とデータを前記第3の鍵で暗号化して得られた第4の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し手段と、

前記第2の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第2の鍵のうちから定められた順番に従い選択した一つ用いて、前記第2の情報のうちから定められた順番に従い選択した一つの暗号化された第1の鍵を復号するとともに、少なくともこの復号結果と前記第3の情報とをもとにして、前記復号により得られたこの第1の鍵が正しいものであるか否かを判定し、正しいものと判定された第1の鍵が得られるまで前記選択および前記判定を繰り返す第1の復号手段と、

この第1の復号手段により正しいものとして得られた前記第1の鍵を用いて前記第3の鍵を復号して得る第2の復号手段と、

この第2の復号手段に得られた前記第3の鍵を用いて前記データを復号して得る第3の復号手段とを備えたことを特徴とする復号装置。

【請求項11】前記第3の情報は、前記第1の鍵を前記第1の鍵自身で暗号化して得られた情報であり、前記第1の復号手段は、前記記憶手段に記憶されている前記第2の鍵の一つを用いて前記第2の情報のうちの一つを復号して得られた鍵と、この鍵を用いて前記前記第3の情報を復号して得られた鍵とが一致した場合に、この鍵が正しい第1の鍵であると判定するものであることを特徴とする請求項8ないし10のいずれか1項に記載の復号装置。

【請求項12】前記データは、鍵情報、文書、音声、画像およびプログラムのうちの少なくとも1つを含むものであることを特徴とする請求項8ないし11のいずれか1項に記載の復号装置。

【請求項13】データを第1の鍵で暗号化して得られた第1の情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化して得られた第2の情報と鍵判定に用いる第3の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出し、前記第2の鍵のうちから定められた順番に従い選択した一つ用いて、前記第2の情報のうちから定められた順番に従い選択した一つの暗号化された第1の鍵を復号するとともに、少なくともこの復号結果と前記第3の情報とをもとにして、前記復号により得られたこの第1の鍵が正しいものであるか否かを判定し、正しいものと判定された第1の鍵が得られるまで前記選択および前記判定を繰り返し、正しいものとして得られた前記第1の鍵を用いて前記データを復号して得ることを特徴とする復号方法。

【請求項14】記録媒体から少なくとも読み出された、データを第1の鍵で暗号化して得られた第1の情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化して得られた第2の情報と鍵判定に用いる第3の情報をと、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のCPUバスを介さずに接続された第1のユニットから計算機のCPUバスを介して第2のユニットに伝えるとともに、少なくとも前記第2および第3の情報については、外部から取得されることなく安全に伝え、

前記第2のユニットにて、前記第2の鍵のうちから定められた順番に従い選択した一つ用いて、前記第2の情報のうちから定められた順番に従い選択した一つの暗号化された第1の鍵を復号するとともに、少なくともこの復号結果と前記第3の情報とをもとにして、前記復号により得られたこの第1の鍵が正しいものであるか否かを判定し、正しいものと判定された第1の鍵が得られるまで前記選択および前記判定を繰り返し、正しいものとして得られた前記第1の鍵を用いて前記データを復号して得ることを特徴とする復号方法。

【請求項15】第3の鍵を第1の鍵で暗号化して得られた第1の情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化して得られた第2の情報と鍵判定に用いる第3の情報とデータを前記第3の鍵で暗号化して得られた第4の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し、前記第2の鍵のうちから定められた順番に従い選択した一つ用いて、前記第2の情報のうちから定められた順番に従い選択した一つの暗号化された第1の鍵を復号するとともに、少なくともこの復号結果と前記第3の情報とをもとにして、前記復号により得られたこの第1の鍵が正しいものであるか否かを判定し、正しいものと判定された第1の鍵が得られるまで前記選択および前記判定を繰り返し、

正しいものとして得られた前記第1の鍵を用いて前記第3の鍵を復号して得、得られた前記第3の鍵を用いて前記データを復号して得ることを特徴とする復号方法。

【請求項16】記録媒体から少なくとも読み出された、データを第1の鍵で暗号化して得られた第1の情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化して得られた第2の情報と鍵判定に用いる第3の情報が、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のCPUバスを介さずに接続されたバス転送用ユニットから計算機のCPUバスを介して伝えられ、これら情報をもとに前記データを復号する復号化ユニット装置であって、前記バス転送用ユニットとの間で前記計算機のCPUバスを介して、少なくとも前記第2および第3の情報を外部から取得されることなく安全に受け渡すための手

段と、

前記第2の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第2の鍵のうちから定められた順番に従い選択した一つを用いて、前記第2の情報のうちから定められた順番に従い選択した一つの暗号化された第1の鍵を復号するとともに、少なくともこの復号結果と前記第3の情報とをもとにして、前記復号により得られたこの第1の鍵が正しいものであるか否かを判定し、正しいものと判定された第1の鍵が得られるまで前記選択および前記判定を繰り返す第1の復号手段と、この第1の復号手段により正しいものとして得られた前記第1の鍵を用いて前記データを復号して得る第2の復号手段とを備えたことを特徴とする復号化ユニット装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ディジタル記録されたデータに対して記録媒体からのコピーを防止するための暗号化方法、復号方法、記録再生装置、復号装置、復号化ユニット装置、記録媒体、記録媒体の製造方法および鍵の管理方法に関する。

【0002】

【従来の技術】従来、ディジタル化された情報（例えば、文書、音声、画像、プログラムなど）を記録する媒体として、音声や画像の記録媒体ではコンパクトディスクやレーザーディスクがある。また、コンピュータなどのプログラムやデータの記録媒体には、フロッピーディスクやハードディスクがある。また、これら記録媒体に加えて、大容量記録媒体であるDVD（ディジタルビデオディスク）が開発されている。

【0003】上記のような種々のディジタル記録媒体において、記録するときにそのままのディジタルデータ（圧縮や符号化等されデコード可能なものも含む）を記録しているため、記録されたデータを他の媒体にコピーすることは、例えば音質や画質の損失なしに、かつ容易にコピーすることが可能であり、複製を大量に作り出すことができ、著作権の侵害など問題があった。

【0004】

【発明が解決しようとする課題】上述したように、ディジタル記録媒体からコピーする場合、音質や画質の劣化がなく、マスターの音質や画質を保ったままコピーすることができる。このため、海賊版と呼ばれる不正なコピーにより、著作権を払うことなくメディアを販売する不法な行為が可能となるなどの問題があった。

【0005】本発明は、上記事情を考慮してなされたもので、ディジタル記録された記録媒体からの不正なコピーを防止するための暗号化方法、復号方法、記録再生装置、復号装置、復号化ユニット装置、記録媒体、記録媒体の製造方法および鍵の管理方法を提供することを目的

とする。

【0006】

【課題を解決するための手段】本発明（請求項1）に係る暗号化方法は、第1の鍵でデータを暗号化し、前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化することを特徴とする。

【0007】本発明（請求項2）に係る記録媒体は、データを第1の鍵で暗号化した情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化した情報とを少なくとも記録したことを特徴とする。

【0008】本発明（請求項3）に係る記録媒体の製造方法は、データを第1の鍵で暗号化した情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化した情報とを同一の記録媒体内に少なくとも記録することを特徴とする。

【0009】本発明（請求項4）に係る復号方法は、データを第1の鍵で暗号化した情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化した情報とを少なくとも入力し、前記第2の鍵の少なくとも一つを用いて前記第1の鍵を復号して得て、得られた第1の鍵が正しいものであることを所定の方法により判定した後に、この第1の鍵を用いて前記データを復号して得ることを特徴とする。

【0010】本発明（請求項5）に係る復号装置は、データを第1の鍵で暗号化した情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化した情報とを少なくとも入力する入力手段と、前記第2の鍵の少なくとも一つを記憶する記憶手段と、この記憶手段内の前記第2の鍵の少なくとも一つを用いて前記入力手段から入力された情報に基づいて前記第1の鍵を復号して得て、得られた第1の鍵が正しいものであることを所定の方法により判定した後に、この第1の鍵を用いて前記データを復号して得る復号手段とを備えたことを特徴とする。

【0011】本発明（請求項6）に係る記録再生装置は、データを第1の鍵で暗号化した情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化した情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し手段と、前記第2の鍵の少なくとも一つを記憶する記憶手段と、この記憶手段内の前記第2の鍵の少なくとも一つを用いて前記読み出し手段から読み出された情報に基づいて前記第1の鍵を復号して得て、得られた第1の鍵が正しいものであることを所定の方法により判定した後に、この第1の鍵を用いて前記データを復号して得る復号手段とを備えたことを特徴とする。

【0012】本発明（請求項7）に係る鍵の管理方法は、第1の管理者に予め定められた複数の第2の鍵を少なくとも保管させ、第2の管理者にデータを第1の鍵で暗号化した情報と前記第1の鍵を前記予め定められた複

数の第2の鍵でそれぞれ暗号化した情報とを少なくとも管理させ、第3の管理者に前記第2の鍵の少なくとも1つを管理させることを特徴とする。

【0013】本発明によれば、複数の第2の鍵のうちの少なくとも1つを持つ正当なもののみが、第1の鍵を得ることができ、従って第1の鍵で暗号化されたデータのプレーンデータを得ることができる。

【0014】この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【0015】本発明（請求項8）に係る復号装置は、データを第1の鍵で暗号化して得られた第1の情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化して得られた第2の情報と鍵判定に用いる第3の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し手段と、前記第2の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第2の鍵のうちから定められた順番に従い選択した一つを用いて、前記第2の情報のうちから定められた順番に従い選択した一つの暗号化された第1の鍵を復号するとともに、少なくともこの復号結果と前記第3の情報とをもとにして、前記復号により得られたこの第1の鍵が正しいものであるか否かを判定し、正しいものと判定された第1の鍵が得られるまで前記選択および前記判定を繰り返す第1の復号手段と、この第1の復号手段により正しいものとして得られた前記第1の鍵を用いて前記データを復号して得る第2の復号手段とを備えたことを特徴とする。

【0016】本発明（請求項9）は、記録媒体から少なくとも読み出された、データを第1の鍵で暗号化して得られた第1の情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化して得られた第2の情報と鍵判定に用いる第3の情報とを、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のCPUバスを介さずに接続された第1のユニットから計算機のCPUバスを介して第2のユニットに伝え、前記第2のユニットにおいて少なくとも前記データの復号を行う復号装置であって、前記第1のユニットは、前記計算機のCPUバスを介して前記第2のユニットへ、前記第1、第2および第3の情報を伝えるときに、少なくとも前記第2および第3の情報については、外部から取得されることなく安全に伝えるための手段を備え、前記第2のユニットは、前記計算機のCPUバスを介して前記第1のユニットから、前記第1、第2および第3の情報を受け取るとともに、少なくとも前記第2および第3の情報については、外部から取得されることなく安全に受け取るための手段と、前記第2の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第2の鍵のうちから定められた順番に従い選択した一つを用いて、前記第2の情報のうちから定められた順

番に従い選択した一つの暗号化された第1の鍵を復号するとともに、少なくともこの復号結果と前記第3の情報とをもとにして、前記復号により得られたこの第1の鍵が正しいものであるか否かを判定し、正しいものと判定された第1の鍵が得られるまで前記選択および前記判定を繰り返す第1の復号手段と、この第1の復号手段により正しいものとして得られた前記第1の鍵を用いて前記データを復号して得る第2の復号手段とを備えたことを特徴とする。

【0017】本発明（請求項10）に係る復号装置は、第3の鍵を第1の鍵で暗号化して得られた第1の情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化して得られた第2の情報と鍵判定に用いる第3の情報とデータを前記第3の鍵で暗号化して得られた第4の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し手段と、前記第2の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第2の鍵のうちから定められた順番に従い選択した一つを用いて、前記第2の情報のうちから定められた順番に従い選択した一つの暗号化された第1の鍵を復号するとともに、少なくともこの復号結果と前記第3の情報とをもとにして、前記復号により得られたこの第1の鍵が正しいものであるか否かを判定し、正しいものと判定された第1の鍵が得られるまで前記選択および前記判定を繰り返す第1の復号手段と、この第1の復号手段により正しいものとして得られた前記第1の鍵を用いて前記第3の鍵を復号して得る第2の復号手段と、この第2の復号手段に得られた前記第3の鍵を用いて前記データを復号して得る第3の復号手段とを備えたことを特徴とする。

【0018】本発明は、記録媒体から少なくとも読み出された、第3の鍵を第1の鍵で暗号化して得られた第1の情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化して得られた第2の情報と鍵判定に用いる第3の情報とデータを前記第3の鍵で暗号化して得られた第4の情報とを、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のCPUバスを介さずに接続された第1のユニットから計算機のCPUバスを介して第2のユニットに伝え、前記第2のユニットにおいて少なくとも前記データの復号を行う復号装置であって、前記第1のユニットは、前記計算機のCPUバスを介して前記第2のユニットへ、前記第1、第2、第3および第4の情報を伝えるときに、少なくとも前記第2および第3の情報については、外部から取得されることなく安全に伝えるための手段を備え、前記第2のユニットは、前記計算機のCPUバスを介して前記第1のユニットから、前記第1、第2、第3および第4の情報を受け取るとともに、少なくとも前記第2および第3の情報については、外部から取得されることなく安全に受け取るための手段と、前記第2の鍵の少なくと

も一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第2の鍵のうちから定められた順番に従い選択した一つ用いて、前記第2の情報のうちから定められた順番に従い選択した一つの暗号化された第1の鍵を復号するとともに、少なくともこの復号結果と前記第3の情報とをもとにして、前記復号により得られたこの第1の鍵が正しいものであるか否かを判定し、正しいものと判定された第1の鍵が得られるまで前記選択および前記判定を繰り返す第1の復号手段と、この第1の復号手段により正しいものとして得られた前記第1の鍵を用いて前記第3の鍵を復号して得る第2の復号手段と、この第2の復号手段に得られた前記第3の鍵を用いて前記データを復号して得る第3の復号手段とを備えたことを特徴とする。

【0019】好ましくは、前記第3の情報は、前記第1の鍵を前記第1の鍵自身で暗号化して得られた情報であり、前記第1の復号手段は、前記記憶手段に記憶されている前記第2の鍵の一つを用いて前記第2の情報のうちの一つを復号して得られた鍵と、この鍵を用いて前記前記第3の情報を復号して得られた鍵とが一致した場合に、この鍵が正しい第1の鍵であると判定するものである。

【0020】好ましくは、前記データは、鍵情報、文書、音声、画像およびプログラムのうちの少なくとも一つを含むものである。

【0021】本発明（請求項13）に係る復号方法は、データを第1の鍵で暗号化して得られた第1の情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化して得られた第2の情報と鍵判定に用いる第3の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出し、前記第2の鍵のうちから定められた順番に従い選択した一つ用いて、前記第2の情報のうちから定められた順番に従い選択した一つの暗号化された第1の鍵を復号するとともに、少なくともこの復号結果と前記第3の情報とをもとにして、前記復号により得られたこの第1の鍵が正しいものであるか否かを判定し、正しいものと判定された第1の鍵が得られるまで前記選択および前記判定を繰り返し、正しいものとして得られた前記第1の鍵を用いて前記データを復号して得ることを特徴とする。

【0022】本発明（請求項14）に係る復号方法は、記録媒体から少なくとも読み出された、データを第1の鍵で暗号化して得られた第1の情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化して得られた第2の情報と鍵判定に用いる第3の情報とを、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のCPUバスを介さずに接続された第1のユニットから計算機のCPUバスを介して第2のユニットに伝えたとともに、少なくとも前記第2および第3の情報については、外部から取得されることなく安全

に伝え、前記第2のユニットにて、前記第2の鍵のうちから定められた順番に従い選択した一つ用いて、前記第2の情報のうちから定められた順番に従い選択した一つの暗号化された第1の鍵を復号するとともに、少なくともこの復号結果と前記第3の情報とをもとにして、前記復号により得られたこの第1の鍵が正しいものであるか否かを判定し、正しいものと判定された第1の鍵が得られるまで前記選択および前記判定を繰り返し、正しいものとして得られた前記第1の鍵を用いて前記データを復号して得ることを特徴とする。

【0023】本発明（請求項15）に係る復号方法は、第3の鍵を第1の鍵で暗号化して得られた第1の情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化して得られた第2の情報と鍵判定に用いる第3の情報とデータを前記第3の鍵で暗号化して得られた第4の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し、前記第2の鍵のうちから定められた順番に従い選択した一つ用いて、前記第2の情報のうちから定められた順番に従い選択した一つの暗号化された第1の鍵を復号するとともに、少なくともこの復号結果と前記第3の情報とをもとにして、前記復号により得られたこの第1の鍵が正しいものであるか否かを判定し、正しいものと判定された第1の鍵が得られるまで前記選択および前記判定を繰り返し、正しいものとして得られた前記第1の鍵を用いて前記第3の鍵を復号して得て、得られた前記第3の鍵を用いて前記データを復号して得ることを特徴とする。

【0024】本発明に係る復号方法は、記録媒体から少なくとも読み出された、第3の鍵を第1の鍵で暗号化して得られた第1の情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化して得られた第2の情報と鍵判定に用いる第3の情報とデータを前記第3の鍵で暗号化して得られた第4の情報とを、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のCPUバスを介さずに接続された第1のユニットから計算機のCPUバスを介して第2のユニットに伝えたとともに、少なくとも前記第2および第3の情報については、外部から取得されることなく安全に伝え、前記第2のユニットにて、前記第2の鍵のうちから定められた順番に従い選択した一つ用いて、前記第2の情報のうちから定められた順番に従い選択した一つの暗号化された第1の鍵を復号するとともに、少なくともこの復号結果と前記第3の情報とをもとにして、前記復号により得られたこの第1の鍵が正しいものであるか否かを判定し、正しいものと判定された第1の鍵が得られるまで前記選択および前記判定を繰り返し、正しいものとして得られた前記第1の鍵を用いて前記第3の鍵を復号して得て、得られた前記第3の鍵を用いて前記データを復号して得ることを特徴とする。

【0025】本発明（請求項16）は、記録媒体から少



なくとも読み出された、データを第1の鍵で暗号化して得られた第1の情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化して得られた第2の情報と鍵判定に用いる第3の情報とが、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のCPUバスを介さずに接続されたバス転送用ユニットから計算機のCPUバスを介して伝えられ、これら情報をもとに前記データを復号する復号化ユニット装置であって、前記バス転送用ユニットとの間で前記計算機のCPUバスを介して、少なくとも前記第2および第3の情報を外部から取得されることなく安全に受け渡すための手段と、前記第2の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第2の鍵のうちから定められた順番に従い選択した一つ用いて、前記第2の情報のうちから定められた順番に従い選択した一つの暗号化された第1の鍵を復号するとともに、少なくともこの復号結果と前記第3の情報とをもとにして、前記復号により得られたこの第1の鍵が正しいものであるか否かを判定し、正しいものと判定された第1の鍵が得られるまで前記選択および前記判定を繰り返す第1の復号手段と、この第1の復号手段により正しいものとして得られた前記第1の鍵を用いて前記データを復号して得る第2の復号手段とを備えたことを特徴とする。

【0026】本発明は、記録媒体から少なくとも読み出された、第3の鍵を第1の鍵で暗号化して得られた第1の情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化して得られた第2の情報と鍵判定に用いる第3の情報とデータを前記第3の鍵で暗号化して得られた第4の情報とが、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のCPUバスを介さずに接続されたバス転送用ユニットから計算機のCPUバスを介して伝えられ、これら情報をもとに前記データを復号する復号化ユニット装置であって、前記バス転送用ユニットとの間で前記計算機のCPUバスを介して、少なくとも前記第2および第3の情報を外部から取得されることなく安全に受け渡すための手段と、前記第2の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第2の鍵のうちから定められた順番に従い選択した一つ用いて、前記第2の情報のうちから定められた順番に従い選択した一つの暗号化された第1の鍵を復号するとともに、少なくともこの復号結果と前記第3の情報とをもとにして、前記復号により得られたこの第1の鍵が正しいものであるか否かを判定し、正しいものと判定された第1の鍵が得られるまで前記選択および前記判定を繰り返す第1の復号手段と、この第1の復号手段により正しいものとして得られた前記第1の鍵を用いて前記第3の鍵を復号して得る第2の復号手段と、この第2の復号手段に得られた前記第3の鍵を用いて前記データを復号して得る第3の復

号手段とを備えたことを特徴とする。

【0027】本発明に係る記録媒体は、データを第1の鍵で暗号化した情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化した情報と鍵判定に用いる情報（例えば、前記第1の鍵を前記第1の鍵自身で暗号化した情報）とを少なくとも記録したことを特徴とする。

【0028】本発明に係る記録媒体は、第3の鍵を第1の鍵で暗号化した情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化した情報とデータを前記第3の鍵で暗号化した情報とを少なくとも記録したことを特徴とする。

【0029】本発明に係る記録媒体は、第3の鍵を第1の鍵で暗号化した情報と前記第1の鍵を予め定められた複数の第2の鍵でそれぞれ暗号化した情報と鍵判定に用いる情報（例えば、前記第1の鍵を前記第1の鍵自身で暗号化した情報）とデータを前記第3の鍵で暗号化した情報とを少なくとも記録したことを特徴とする。

【0030】本発明によれば、複数の第2の鍵のうちの少なくとも一つを持つ正当なもののみが、第1の鍵を得ることができ、従って第1の鍵で暗号化されたデータのプレーンデータを得ることができる。この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【0031】また、本発明によれば、暗号化ユニットと復号化ユニットとを接続する信号線に流れるデータを保存したとしても、該データは暗号化されたものであり、また、該データを暗号化するために必要な情報は、乱数をもとにして生成されるものであって、後に再現できないために、たとえ、復号ユニット内の第2の鍵（マスターキー）が破られたとしても、保存したデータを再生または利用することはできない。この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。また、本発明によれば、暗号化ユニットおよび復号化ユニットは、デジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、たとえ暗号が破られたとしても、暗号化ユニットおよび復号化ユニットを交換するだけで良い。

【0032】また、本発明1は、所定の第1のセッションキーで暗号化されたデジタル・データと、予め定められたマスターキーで暗号化された第1のセッションキーとを記録した記録媒体から該デジタル・データの平文を得るための復号方法であって、復号化ユニットにて、所定の乱数をもとにして第2のセッションキーを生成し、生成された第2のセッションキーを前記マスターキーで復号し、復号化ユニットから暗号化ユニットへ、前記マスターキーで復号された第2のセッションキーを伝送し、暗号化ユニットにて、伝送された前記マスターキーで復号された第2のセッションキーを、前記マスターキーで暗号化して、前記第2のセッションキーを取り出

し、暗号化ユニットにて、取り出された前記第2のセッションキーを用いて、前記記録媒体から読み出された前記マスターキーで暗号化された第1のセッションキーを暗号化し、暗号化ユニットから復号化ユニットへ、第2のセッションキーを用いて暗号化された、前記マスターキーで暗号化された第1のセッションキーを伝送し、復号化ユニットにて、伝送された前記第2のセッションキーを用いて暗号化された、前記マスターキーで暗号化された第1のセッションキーを、前記第2のセッションキーを用いて復号し、前記マスターキーで暗号化された第1のセッションキーを取り出し、さらに取り出された前記マスターキーで暗号化された第1のセッションキーを、前記マスターキーで復号して、前記第1のセッションキーを取り出し、取り出された前記第1のセッションキーを用いて、前記記録媒体から読み出された前記第1のセッションキーで暗号化されたデジタル・データを復号して、前記デジタル・データの平文を得ることを特徴とする。

【0033】本発明2は、所定の第1のセッションキーで暗号化されたデジタル・データと、予め定められた複数のマスターキーのうちの所定のマスターキーで暗号化された第1のセッションキーと、第1のセッションキー自身で暗号化された第1のセッションキーとを記録した記録媒体から該デジタル・データの平文を得るための復号方法であって、復号化ユニットにて、所定の乱数をもとにして第2のセッションキーを生成し、生成された第2のセッションキーを予め定められたマスターキーで復号し、復号化ユニットから暗号化ユニットへ、前記予め定められたマスターキーで復号された第2のセッションキーを伝送し、暗号化ユニットにて、伝送された前記予め定められたマスターキーで復号された第2のセッションキーを、前記予め定められたマスターキーで暗号化して、前記第2のセッションキーを取り出し、暗号化ユニットにて、取り出された前記第2のセッションキーを用いて、前記記録媒体から読み出された前記所定のマスターキーで暗号化された第1のセッションキーを暗号化するとともに、取り出された前記第2のセッションキーを用いて、前記記録媒体から読み出された前記第1のセッションキー自身で暗号化された第1のセッションキーを暗号化し、暗号化ユニットから復号化ユニットへ、第2のセッションキーを用いて暗号化された、前記所定のマスターキーで暗号化された第1のセッションキーを伝送するとともに、第2のセッションキーを用いて暗号化された、前記第1のセッションキー自身で暗号化された第1のセッションキーを伝送し、復号化ユニットにて、伝送された前記第2のセッションキーを用いて暗号化された、前記マスターキーで暗号化された第1のセッションキーを、前記第2のセッションキーを用いて復号し、前記所定のマスターキーで暗号化された第1のセッションキーを取り出すとともに、伝送された前記第2の

セッションキーを用いて暗号化された、前記第1のセッションキー自身で暗号化された第1のセッションキーを、前記第2のセッションキーを用いて復号し、前記第1のセッションキー自身で暗号化された第1のセッションキーを取り出し、復号化ユニットにて、取り出された前記所定のマスターキーで暗号化された第1のセッションキーを、予め定められた複数のマスターキーのうちのいずれかで復号した第1のセッションキー候補と、取り出された前記第1のセッションキー自身で暗号化された第1のセッションキーを、該第1のセッションキー候補で復号したものとが一致した場合に、該第1のセッションキー候補を前記所定の第1のセッションキーとし、得られた前記第1のセッションキーを用いて、前記記録媒体から読み出された前記第1のセッションキーで暗号化されたデジタル・データを復号して、前記デジタル・データの平文を得ることを特徴とする。

【0034】本発明3は、所定の第1のセッションキーで暗号化されたデジタル・データと、予め定められた複数のマスターキーで夫々暗号化された第1のセッションキーと、第1のセッションキー自身で暗号化された第1のセッションキーとを記録した記録媒体から該デジタル・データの平文を得るための復号方法であって、復号化ユニットにて、所定の乱数をもとにして第2のセッションキーを生成し、生成された第2のセッションキーを予め定められたマスターキーで復号し、復号化ユニットから暗号化ユニットへ、予め定められたマスターキーで復号された第2のセッションキーを伝送し、暗号化ユニットにて、伝送された予め定められたマスターキーで復号された第2のセッションキーを、予め定められたマスターキーで暗号化して、前記第2のセッションキーを取り出し、暗号化ユニットにて、取り出された前記第2のセッションキーを用いて、前記記録媒体から読み出された前記マスターキーで暗号化された第1のセッションキーを暗号化するとともに、取り出された前記第2のセッションキーを用いて、前記記録媒体から読み出された前記第1のセッションキー自身で暗号化された第1のセッションキーを暗号化し、暗号化ユニットから復号化ユニットへ、第2のセッションキーを用いて暗号化された、前記マスターキーで暗号化された第1のセッションキーを伝送するとともに、第2のセッションキーを用いて暗号化された、前記第1のセッションキー自身で暗号化された第1のセッションキーを伝送し、復号化ユニットにて、伝送された前記第2のセッションキーを用いて暗号化された、前記マスターキーで暗号化された第1のセッションキーを、前記第2のセッションキーを用いて復号し、前記マスターキーで暗号化された第1のセッションキーを取り出すとともに、伝送された前記第2のセッションキーを用いて暗号化された、前記第1のセッションキー自身で暗号化された第1のセッションキーを、前記第2のセッションキーを用いて復号し、前記第1のセッ

セッションキー自身で暗号化された第1のセッションキーを取り出し、復号化ユニットにて、取り出された前記マスターキーで暗号化された第1のセッションキーを、予め定められたマスターキーで復号した第1のセッションキー候補と、取り出された前記第1のセッションキー自身で暗号化された第1のセッションキーを、該第1のセッションキー候補で復号したものとが一致した場合に、該第1のセッションキー候補を前記所定の第1のセッションキーとし、得られた前記第1のセッションキーを用いて、前記記録媒体から読み出された前記第1のセッションキーで暗号化されたデジタル・データを復号して、前記デジタル・データの平文を得ることを特徴とする。

【0035】本発明4は、所定の第1のセッションキーで暗号化されたデジタル・データと、予め定められた複数のマスターキーで夫々暗号化された第1のセッションキーと、第1のセッションキー自身で暗号化された第1のセッションキーとを記録した記録媒体から該デジタル・データの復号に用いる第1のセッションキーを得るための復号方法であって、前記マスターキーで暗号化された第1のセッションキーを、前記複数のマスターキーのうちの予め定められたものを復号して第1のセッションキー候補を生成し、生成された前記第1のセッションキー候補を用いて、前記第1のセッションキー自身で暗号化された第1のセッションキーを復号し、前記第1のセッションキー候補と、該第1のセッションキー候補を用いて復号された、前記第1のセッションキー自身で暗号化された第1のセッションキーとを比較し、前記比較にて一致した場合に、前記第1のセッションキー候補を前記所定の第1のセッションキーとして決定することを特徴とする。

【0036】本発明5は、上記発明1ないし3のいずれか1つの発明において、前記暗号化ユニットおよび前記復号化ユニットは、それぞれ、独立して形成された集積回路素子であることを特徴とする。

【0037】本発明6は、上記発明1ないし3のいずれか1つの発明において、前記暗号化ユニットと前記復号化ユニットとの間で行われる伝送は、CPU BUSを用いて行われることを特徴とする。

【0038】本発明7は、上記発明1ないし3のいずれか1つの発明において、前記所定の乱数は、少なくとも前記記録媒体を再生する度に变化するものであることを特徴とする。

【0039】本発明8は、上記発明1ないし3のいずれか1つの発明において、前記所定の乱数は、所定のタイミングで得られる時間情報をもとにして生成されることを特徴とする。

【0040】所定のタイミングは、例えば、前記記録媒体がその駆動装置に装着されたタイミングである。

【0041】本発明9は、上記発明1ないし4のいずれか1つの発明において、前記データは、鍵情報、文書、

音声、画像およびプログラムのうちの少なくとも1つを含むものであることを特徴とする。

【0042】本発明10は、所定の第1のセッションキーで暗号化されたデジタル・データと、予め定められたマスターキーで暗号化された第1のセッションキーとを記録した記録媒体から該デジタル・データの平文を得るための復号装置であって、復号化ユニット内に設けられ、所定の条件に応じて異なる第2のセッションキーを生成する第2のセッションキー生成手段と、生成された前記第2のセッションキーを前記復号化ユニット内で前記マスターキーにて復号し、このデータを暗号化ユニット内へ伝送し、前記暗号化ユニット内で前記マスターキーで暗号化することにより前記第2のセッションキーを取り出す手段と、この手段により取り出された第2のセッションキーを用いて、前記記録媒体から読み出された前記マスターキーで暗号化された前記第1のセッションキーを暗号化し前記復号化ユニットへ伝送する手段と、この手段により復号化ユニット内へ伝送された暗号化された第1のセッションキーを前記復号化ユニット内で生成された第2のセッションキーを用いて復号した後にさらに前記マスターキーを用いて復号して前記第1のセッションキーを得る手段と、この手段により得られた前記第1のセッションキーを用いて、前記記録媒体から読み出された前記第1のセッションキーで暗号化されたデジタル・データを復号して、前記デジタル・データの平文を得る手段とを備えたことを特徴とする。

【0043】本発明11は、上記発明10において、前記第2のセッションキー生成手段は、前記記録媒体の復号操作を行うごとに、あるいは時間情報に応じて異なる第2のセッションキーを生成することを特徴とする。

【0044】本発明12に係る記録媒体は、所定の第1のセッションキーで暗号化されたデジタル・データと、予め定められた複数のマスターキーで夫々暗号化された第1のセッションキーと、第1のセッションキー自身で暗号化された第1のセッションキーとを記録したことを特徴とする。

【0045】記録媒体は、例えば、DVD、CD-ROM、フロッピーディスク、ハードディスクなど、種々のものに適用可能である。

【0046】なお、以上の装置に係る各発明は、それぞれ、方法に係る発明や記憶媒体に係る発明としても成立し、以上の方法に係る各発明は、それぞれ、装置に係る発明や記憶媒体に係る発明としても成立する。

【0047】本発明によれば、暗号化ユニットと復号化ユニットとを接続する信号線に流れるデータを保存したとしても、該データは暗号化されたものであり、また、該データを暗号化するために必要な情報は、乱数をもとにして生成されるものであって、後に再現できないために、たとえ、復号ユニット内のマスターキーが破れたとしても、保存したデータを再生または利用することは

できない。

【0048】この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【0049】また、本発明によれば、暗号化ユニットおよび復号化ユニットは、デジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、たとえ暗号が破られたとしても、暗号化ユニットおよび復号化ユニットを交換するだけで良い。

【0050】また、本発明によれば、記録媒体に、所定の第1のセッションキーで暗号化されたデジタル・データと、予め定められた複数のマスターキーのうちの所定のマスターキーで暗号化された第1のセッションキーと、第1のセッションキー自身で暗号化された第1のセッションキーとを記録しておくことにより、前記所定のマスターキーが複数のマスターキーのうちのいずれであっても、複数のマスターキーを持つ復号化ユニットにより、第1のセッションキーを取り出し、この第1のセッションキーにより、データを復号することができる。

【0051】また、本発明によれば、記録媒体に、所定の第1のセッションキーで暗号化されたデジタル・データと、予め定められた複数のマスターキーで夫々暗号化された第1のセッションキーと、第1のセッションキー自身で暗号化された第1のセッションキーとを記録しておくことにより、前記複数のマスターキーのうちのいずれかを少なくとも1つでも持つ復号化ユニットにより、第1のセッションキーを取り出し、この第1のセッションキーにより、データを復号することができる。

【0052】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【0053】本実施形態では、あるデータaを鍵Kを用いて暗号化する操作を $E_K(a)$ と表現し、あるデータaを鍵Kを用いて復号化する操作を $D_K(a)$ と表現する。この表現を用いることにより、例えば、あるデータaを鍵Kを用いて暗号化し復号する操作は、 $D_K(E_K(a))$ で表される。

【0054】また、本実施形態では、あるデータをまず復号化し、その後、復号化されたデータを暗号化してもとのデータに戻すことがある。これは、暗号の性質上、データの復号化に暗号化と同等の作用があることに基づいている。つまり、復号化したデータをもとに戻すためには復号化に用いた鍵がわからなければならず、鍵が判れば復号化したデータを暗号化することにより最初に復号化したデータが得られる。この操作は、暗号鍵をxとしデータをyとすれば、 $E_x(D_x(y)) = y$ で表される。

【0055】本実施形態では、DVDに記録された、MPEG2というデータ圧縮規格に従って圧縮され暗号化

された画像データを、読み出し復号しデコードして再生するシステムを例にとって説明する。

【0056】（第1の実施形態）以下、第1の実施形態について説明する。

【0057】図1は、本発明の第1の実施形態に係るシステムの構成を示すブロック図である。また、本実施形態の動作の一例を図2のフローチャートに示す。

【0058】本実施形態に係るシステムは、パーソナル・コンピュータなどの計算機内に備えられた再生に用いるCPU（図示せず）のいわゆるCPU BUSに接続されるものであり、暗号化されたデータ（後述するESK(Data)）がCPU BUS上を流れる構成を有するものである。なお、図1では、再生に用いるCPUに関する部分のみ示している。

【0059】図1に示すように、本実施形態に係るシステムは、DVD101からデータを読み出すDVD駆動装置（図示せず）、このDVD駆動装置にCPU BUSを介さずに接続されたまたはDVD駆動装置に内蔵された暗号化ユニット107、復号化ユニット114を備えている。

【0060】暗号化ユニット107と復号化ユニット114は、CPU BUS110に接続されている。復号化ユニット114からのデータの出力は、CPU BUS以外の例えばI/Oポート等を通じて行われる。つまり、本実施形態では、データの入出力はCPU BUSを介さずに行われるが、暗号化ユニット107と復号化ユニット114との間でのデータ転送には、CPU BUSが用いられる。

【0061】暗号化ユニット107は、復調/誤り訂正回路117、復調/誤り訂正回路118、暗号化回路104を備えている。図1中で、暗号化ユニット107内には、2つの暗号化回路104を示しているが、実際には1つの暗号化回路であるものとする。暗号化ユニット107は、独立した1つのICチップとして形成されるものとする。なお、復調/誤り訂正回路117および復調/誤り訂正回路118は、暗号化ユニット107内には備えず、その前段のユニット等の側（DVD駆動装置内）に備えられる場合もある。

【0062】一方、復号化ユニット114は、復号化回路112、第2のセッションキー $S_K'$ を生成するセッションキー生成回路111を備えている。また、本実施形態では、復号化ユニット114内にMPEGのデコード回路115および復号された画像データをデジタルからアナログに変換する変換回路116を備えているものとする。図1中で、復号化ユニット114内には、4つの復号化回路112を示しているが、実際には1つの復号化回路であるものとする。復号化ユニット114は、独立した1つのICチップとして形成されるものとする。

【0063】また、暗号化ユニット107内、および復

号化ユニット114内には、後述するマスターキーが登録されている（作り込まれている）。マスターキーは、利用者が外部から取得できないように、暗号化ユニットのチップ、復号化ユニットのチップそれぞれにおいて、利用者が意図的に取り出せないようにチップ内部の秘匿された領域に記録されているものとする。

【0064】なお、全体の制御は図示しない制御部が司るものとする。制御部は例えばプログラムを当該計算機のCPUで実行することにより実現することができる。この制御部による制御の具体例としては、DVDからのデータの読み出しに関する指示、データ伝送先の指定、復号化ユニット114からのデータ出力に関する指示等である。また、この制御部の起動のトリガーは、例えば、ユーザ・インタフェースを介してユーザにより行われる場合と、あるアプリケーションプログラム中のプロセスからかけられる場合などが考えられる。

【0065】本実施形態では、第1のセッションキーを $S_K$ 、第2のセッションキーを $S_K'$ 、マスターキーを $M_K$ 、画像データ（すなわち暗号化された一纏まりのデータ）を $Data$ で表す。これらはいずれも平文である。

【0066】図1中、102は第1のセッションキー $S_K$ をマスターキー $M_K$ を用いて暗号化して生成された $EMK(S_K)$ を、103は画像データ $Data$ を第1のセッションキー $S_K$ を用いて暗号化して生成された $ESK(Data)$ を、105はマスターキー $M_K$ を、106は第2のセッションキー $S_K'$ を、108は第2のセッションキー $S_K'$ をマスターキー $M_K$ を用いて復号した $DMK(S_K')$ を、109はマスターキー $M_K$ を用いて暗号化された第1のセッションキー $EMK(S_K)$ を第2のセッションキー $S_K'$ を用いて暗号化した $ESK'(EMK(S_K))$ を、113は第1のセッションキー $S_K$ をそれぞれ表す。

【0067】図3に示すように、DVD101上で、第1のセッションキー $S_K$ をマスターキー $M_K$ を用いて暗号化して生成された $EMK(S_K)$ は、最内周部分の鍵記録領域（リードインエリア）に、画像データ $Data$ を第1のセッションキー $S_K$ を用いて暗号化して生成された $ESK(Data)$ は、データ記録領域（データエリア）に記録されているものとする。

【0068】以下、図2のフローチャートを参照しながら、本実施形態の動作について説明する。

【0069】ステップS1で、図示しないDVD駆動装置によりDVD101に記録されている、マスターキー $M_K$ を用いて暗号化された第1のセッションキー $EMK(S_K)$ を読み出し、暗号ユニット107内に取り込む。その際、復調／誤り訂正回路117により復調、データ中の誤り訂正が行われる。

【0070】一方、ステップS2で、復号化ユニット114では、セッションキー生成回路111において、乱

数、例えば時計（図示せず）からの時間情報を入力として第2のセッションキー $S_K'$ を生成する。そして、復号化回路112において、生成された第2のセッションキー $S_K'$ を、マスターキー $M_K$ を用いて復号して $DMK(S_K')$ を生成し、CPU BUS110を通じて暗号化ユニット107に送る。

【0071】上記の乱数を発生するタイミング（例えば時間情報を入力するタイミング）としては、例えば、DVD駆動装置にDVD101が装着されたことを示す信号がアサートされたタイミングを用いることができる。

【0072】あるいは、セッションキー生成回路111は、例えば鍵長分の乱数発生器で構成しても良い。なお、全てのビットが0や1になる可能性のある乱数で鍵を生成する場合は、全てのビットが0や1になることがないようにチェック処理等をする必要がある。

【0073】ステップS3で、暗号ユニット107では、暗号化回路104において、CPU BUS110を通じて受け取った $DMK(S_K')$ を、マスターキー $M_K$ を用いて暗号化する。すなわち、 $EMK(DMK(S_K')) = S_K'$ により、復号化ユニット114内のセッションキー生成回路111で生成された第2のセッションキー $S_K'$ を得ることができる。

【0074】ここで、セッションキー生成回路111で生成された第2のセッションキー $S_K'$ は、CPU BUS110上で盗まれたとしても解らないようにしてある。

【0075】次に、ステップS4で、暗号ユニット107では、上記のようにして得られた第2のセッションキー $S_K'$ を用いて、DVD101に記録された暗号化された第1のセッションキー $EMK(S_K)$ を暗号化して、 $ESK'(EMK(S_K))$ を生成し、これをCPU BUS110を通じて復号化ユニット114へ送る。

【0076】次に、ステップS5で、復号化ユニット114では、復号化回路112において、CPU BUS110を通じて受け取った $ESK'(EMK(S_K))$ を、第2のセッションキー $S_K'$ を用いて復号し、 $DSK'(ESK'(EMK(S_K))) = EMK(S_K)$ を得る。

【0077】さらに、復号化回路112において、得られた $EMK(S_K)$ を、マスターキー $M_K$ を用いて復号し、 $DMK(EMK(S_K)) = S_K$ となり、第1のセッションキー $S_K$ を得ることができる。

【0078】以上のようにして第1のセッションキー $S_K$ を得た後、ステップS6で、図示しないDVD駆動装置によりDVD101に記録されている、第1のセッションキー $S_K$ を用いて暗号化された画像データ $ESK(Data)$ を読み出し、暗号ユニット107内に取り込

む。その際、復調／誤り訂正回路118により復調、データ中の誤り訂正が行われる。そして、 $E_{SK}(Data)$ を、CPU BUS110を通じて暗号化ユニット107に送る。

【0079】次に、ステップS7で、復号化ユニット114では、復号化回路112において、CPU BUS110を通じて受け取った $E_{SK}(Data)$ を、第1のセッションキー $S_K$ を用いて復号し、

$D_{SK}(E_{SK}(Data)) = Data$

となり、暗号化された画像データを復号して、平文の $Data$ を得ることができる。

【0080】そして、例えば復号すべきデータ（すなわち $E_{SK}(Data)$ ）の処理が終了し、あるいは処理の中止を要求されるまで、上記のステップS6とステップS7が繰り返し行われる。

【0081】以上のようにして得られた画像データ $Data$ は、例えばMPEG2というデータ圧縮規格に従って圧縮されている場合にはMPEGデコーダ回路115でデコードされ、そしてD/A変換回路116でアナログ信号に変換された後、図示しないテレビなどの映像装置に送られ、再生される。

【0082】なお、上記のステップS1と、ステップS2およびS3とは、どちらを先に実行しても構わない。

【0083】また、ステップS6とステップS7の実行については、1つの $E_{SK}(Data)$ の単位で逐次行う方法、あるいはステップS6で所定数の $E_{SK}(Data)$ を読み込み、一旦バッファなどへ格納し、次にステップS7でバッファ内の $E_{SK}(Data)$ を復号する方法、あるいはステップS6とステップS7をパイプライン処理的に行う方法などが考えられる。

【0084】また、復号化回路112からMPEGデコーダ回路115に画像データ $E_{SK}(Data)$ を渡す際に、1つの $Data$ の単位で渡しても良いし、所定数の $Data$ の単位で渡しても良い。

【0085】以上のように本実施形態によれば、デジタル化されたデータを暗号化して記録した媒体を再生する場合（暗号化されたデータを復号する場合）に、計算機のCPU BUSに復号されたデータが流れず、また、CPU BUSに流れる暗号化されたデータの復号に必要な第1のセッションキーの暗号化に用いた第2のセッションキー $S_K'$ は、例えば時間情報のようにデータ再生の度に変わる情報をもとに生成されるため、図4のようにCPU BUS110を流れるデータを信号線210からデジタル記憶媒体211に保存したとしても、それを再生または利用することはできない。

【0086】この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【0087】また、本実施形態では、暗号化および復号化に用いる回路は、図1から解るようにDVDなどのデ

ジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、たとえ暗号が破られたとしても、復号化ユニット114（あるいは暗号化ユニット107および復号化ユニット114）を交換するだけで良い。

【0088】なお、本実施形態では、暗号ユニット107は1つの暗号化回路を持つものとしたが、2つの暗号化回路を設けても良い。また、復号化ユニット114は1つの復号化回路を持つものとしたが、2、3、または4つの復号化回路として設けても良い。これらの場合、対応する暗号化回路と復号化回路をセットで独立化しあるいは共用するのが好ましい。

【0089】また、対応する暗号化回路と復号化回路をセットで独立化する場合、独立化した対応する暗号化回路および復号化回路では、他の暗号化回路および復号化回路とは異なる暗号方式を採用しても構わない。

【0090】（第2の実施形態）次に、第2の実施形態について説明する。

【0091】本実施形態では、例えば、予め定めた複数のマスターキーを用意し、そのうちの1つまたは複数のマスターキーを、復号化ユニットのメーカー（あるいはDVDの制作・販売会社）などの所定の単位ごとに割り当てるような場合に好適な例について説明する。

【0092】図5は、本発明の第2の実施形態に係るシステムの構成を示すブロック図である。また、本実施形態の動作の一例を図7および図8のフローチャートに示す。

【0093】本実施形態に係るシステムは、パーソナル・コンピュータなどの計算機内に備えられた再生に用いるCPU（図示せず）のいわゆるCPU BUSに接続されるものであり、暗号化されたデータ（ $E_{SK}(Data)$ ）がCPU BUS上を流れる構成を有するものである。なお、図5では、再生に用いるCPUに関する部分のみ示している。

【0094】図5に示すように、本実施形態に係るシステムは、DVD101からデータの読み出すDVD駆動装置（図示せず）、このDVD駆動装置にCPU BUSを介さずに接続されたまたはDVD駆動装置に内蔵された暗号化ユニット107、復号化ユニット114aを備えている。

【0095】暗号化ユニット107と復号化ユニット114aは、CPU BUS110に接続されている。復号化ユニット114aからのデータの出力は、CPU BUS以外の例えばI/Oポート等を通じて行われる。つまり、本実施形態では、データの入出力はCPU BUSを介さずに行われるが、暗号化ユニット107と復号化ユニット114aとの間でのデータ転送には、CPU BUSが用いられる。

【0096】暗号化ユニット107は、復調／誤り訂正回路117、復調／誤り訂正回路118、暗号化回路104を備えている。図1中で、暗号化ユニット107内

には、2つの暗号化回路104を示しているが、実際には1つの暗号化回路であるものとする。暗号化ユニット107は、独立した1つのICチップとして形成されるものとする。なお、復調/誤り訂正回路117および復調/誤り訂正回路118は、暗号化ユニット107内には備えず、その前段のユニット等の側(DVD駆動装置内)に備えられる場合もある。

【0097】一方、復号化ユニット114aは、復号化回路112、第2のセッションキー $S_K'$ を生成するセッションキー生成回路111、鍵判定回路120を備えている。

【0098】ここで、図6に、鍵判定回路120の一構成例を示す。この鍵判定回路120は、復号化回路112、比較回路121、ゲート回路122を備えている。また、本実施形態では、復号化ユニット114a内にMPEGのデコーダ回路115および復号された画像データをデジタルからアナログに変換する変換回路116を備えているものとする。

【0099】図5および図6中で、復号化ユニット114a内には、鍵判定回路120内の2つの復号化回路112を含めて、全部で5つの復号化回路112を示しているが、実際には1つの復号化回路であるものとする。

【0100】復号化ユニット114aは、独立した1つのICチップとして形成されるものとする。

【0101】また、暗号化ユニット107内、および復号化ユニット114a内には、後述するマスターキーが登録されている(作り込まれている)。マスターキーは、利用者が外部から取得できないように、暗号化ユニットのチップ、復号化ユニットのチップそれぞれにおいて、利用者が意図的に取り出せないようにチップ内部の秘匿された領域に記録されているものとする。

【0102】なお、全体の制御は図示しない制御部が司るものとする。制御部は例えばプログラムを当該計算機のCPUで実行することにより実現することができる。この制御部による制御の具体例としては、DVDからのデータの読み出しに関する指示、データ伝送先の指定、復号化ユニット114aからのデータ出力に関する指示等である。また、この制御部の起動のトリガーは、例えば、ユーザ・インタフェースを介してユーザにより行われる場合と、あるアプリケーションプログラム中のプロセスからかけられる場合などが考えられる。

【0103】本実施形態では、第1のセッションキーを $S_K$ 、第2のセッションキーを $S_K'$ 、 $n$ 種類存在するマスターキーのうちの $t$ 番目のものを $M_{kt}$ (ここで $t=1\sim n$ )、画像データ(ただし、暗号化された一纏まりのデータ)を $Data$ で表す。これらはいずれも平文である。

【0104】図1中、102-1は第1のセッションキー $S_K$ をマスターキー $M_{ki}$ を用いて暗号化して生成された $E_{Sk}(S_K)$ を、102-2は第1のセッションキ

ー $S_K$ を第1のセッションキー $S_K$ 自身で暗号化して生成された $E_{Sk}(S_K)$ を、103は画像データ $Data$ を第1のセッションキー $S_K$ を用いて暗号化して生成された $E_{Sk}(Data)$ を、105はマスターキー $M_{kj}$ を、106は第2のセッションキー $S_K'$ を、108は第2のセッションキー $S_K'$ をマスターキー $M_{kj}$ を用いて復号した $D_{Mkj}(S_K')$ を、109-1はマスターキー $M_{ki}$ を用いて暗号化された第1のセッションキー $E_{Mki}(S_K)$ を第2のセッションキー $S_K'$ を用いて暗号化した $E_{Sk'}(E_{Mki}(S_K))$ を、109-2は第1のセッションキー $S_K$ 自身で暗号化された第1のセッションキー $E_{Sk}(S_K)$ を第2のセッションキー $S_K'$ を用いて暗号化した $E_{Sk'}(E_{Sk}(S_K))$ を、113は第1のセッションキー $S_K$ をそれぞれ表す。

【0105】ここで、DVD101に記録する第1のセッションキー $S_K$ をマスターキー $M_{ki}$ を用いて暗号化して生成された $E_{Mki}(S_K)$ の種類数と、復号化ユニット114a内に持つマスターキー $M_{kj}$ の種類数の設定について、例えば次に示すように幾つかの方法が考えられる。

【0106】(方法1) DVD101には $i$ を $1\sim n$ のいずれかとする1つのマスターキー $E_{Mki}(S_K)$ を記録し、復号化ユニット114a内には $j=1\sim n$ のすべてに対応する $n$ 個のマスターキー $M_{kj}$ を備える。

【0107】(方法2) DVD101には $i=1\sim n$ のすべてに対応する $n$ 個のマスターキー $E_{Mki}(S_K)$ を記録し、復号化ユニット114a内には $j=1\sim n$ のいずれかとする1つのマスターキー $M_{kj}$ を備える。

【0108】(方法3) 上記の(方法2)を拡張したもので、DVD101には $i=1\sim n$ のすべてに対応する $n$ 個のマスターキー $E_{Mki}(S_K)$ を記録し、復号化ユニット114a内には $j=1\sim n$ のうちのから予め選択された $m$ ( $2<m<n$ )種類のものとする $m$ 個のマスターキー $M_{kj}$ を備える。

【0109】なお、具体的な数値例としては、例えば、 $n=100$ あるいは $n=400$ などであり、 $m=2, 3$ , あるいは $4$ 、あるいは $10$ などであるが、これらに限定されるものではない。

【0110】(方法4) 上記の(方法3)においてDVDと復号化ユニットを逆にした例で、DVD101には $i=1\sim n$ のうちのから予め選択された $m$ ( $2<m<n$ )種類のものとする $m$ 個のマスターキー $E_{Mki}(S_K)$ を記録し、復号化ユニット114a内には $j=1\sim n$ のすべてに対応する $n$ 個のマスターキー $M_{kj}$ を備える。

【0111】(方法5) DVD101には $i=1\sim n$ のすべてに対応する $n$ 個のマスターキー $E_{Mki}(S_K)$ を記録し、復号化ユニット114a内には $j=1\sim n$ のすべてに対応する $n$ 個のマスターキー $M_{kj}$ を備える。

【0112】なお、方法3～方法5は、復号のための手

順は同様になる。

【0113】図3に示すように、DVD101上で、第1のセッションキー $S_K$ をマスターキー $M_{ki}$ を用いて暗号化して生成された1個(上記の(方法1)の場合)または複数個(上記の(方法2)～(方法5)の場合)の $EM_{ki}(S_K)$ は、最内周部分の鍵記録領域(リードインエリア)に、画像データDataを第1のセッションキー $S_K$ を用いて暗号化して生成された $ES_K(Data)$ は、データ記録領域(データエリア)に記録されているものとする。

【0114】また、復号化ユニット114内に、 $n$ 個(上記の(方法1)、(方法4)、(方法5)の場合)、または1個(上記の(方法2)の場合)、または $m$ 個(上記の(方法3)の場合)のマスターキー $M_{kj}$ が登録されているものとする。

【0115】なお、暗号化ユニット107内には、予め定められた1つのマスターキーが登録されているものとする。

【0116】以下では、上記の(方法1)、(方法2)、(方法3～方法5)について順次説明する。

【0117】まず、上記の(方法1)の場合について図7および図8のフローチャートを参照しながら本実施形態の動作を説明する。

【0118】ステップS11で、図示しないDVD駆動装置によりDVD101に記録されている、第1のセッションキー $S_K$ 自身で暗号化された第1のセッションキー $ES_K(S_K)$ を読み出し、暗号ユニット107内に取り込む。その際、復調/誤り訂正回路117により復調、データ中の誤り訂正が行われる。

【0119】また、ステップS12で、図示しないDVD駆動装置によりDVD101に記録されている、マスターキー $M_{ki}$ を用いて暗号化された第1のセッションキー $EM_{ki}(S_K)$ ( $i=1\sim n$ のいずれか1つ;ここでは $i$ は未知である)を読み出し、暗号ユニット107内に取り込む。その際、復調/誤り訂正回路117により復調、データ中の誤り訂正が行われる。

【0120】一方、ステップS13で、復号化ユニット114aでは、セッションキー生成回路111において、乱数、例えば時計(図示せず)からの時間情報を入力として第2のセッションキー $S_K'$ を生成する。そして、復号化回路112において、生成された第2のセッションキー $S_K'$ を、マスターキー $M_{kj}$ (ここで $j$ は $1\sim n$ のうち予め定められたもの)を用いて復号して $DM_{kj}(S_K')$ を生成し、CPU BUS110を通じて暗号化ユニット107に送る。

【0121】上記の乱数を発生するタイミング(例えば時間情報を入力するタイミング)としては、例えば、DVD駆動装置にDVD101が装着されたことを示す信号がアサートされたタイミングを用いることができる。

【0122】あるいは、セッションキー生成回路111

は、例えば鍵長分の乱数発生器で構成しても良い。なお、全てのビットが0や1になる可能性のある乱数で鍵を生成する場合は、全てのビットが0や1になることがないようにチェック処理等をする必要がある。

【0123】ステップS14で、暗号ユニット107では、暗号化回路104において、CPU BUS110を通じて受け取った $DM_{kj}(S_K')$ を、マスターキーをマスターキー $M_{kj}$ (ここで $j$ は $1\sim n$ のうち予め定められたもの)を用いて暗号化する。すなわち、 $EM_{kj}(DM_{kj}(S_K'))=S_K'$ により、復号化ユニット114a内のセッションキー生成回路111で生成された第2のセッションキー $S_K'$ を得ることができる。

【0124】ここで、セッションキー生成回路111で生成された第2のセッションキー $S_K'$ は、CPU BUS110上で盗まれたとしても解らないようにしてある。

【0125】次に、ステップS15で、暗号ユニット107では、上記のようにして得られた第2のセッションキー $S_K'$ を用いて、DVD101に記録された暗号化された第1のセッションキー $ES_K(S_K)$ を暗号化して、 $ES_K'(ES_K(S_K))$ を生成し、これをCPU BUS110を通じて復号化ユニット114aへ送る。

【0126】同様に、ステップS16で、暗号ユニット107では、上記のようにして得られた第2のセッションキー $S_K'$ を用いて、DVD101に記録された暗号化された第1のセッションキー $EM_{ki}(S_K)$ を暗号化して、 $ES_K'(EM_{ki}(S_K))$ を生成し、これをCPU BUS110を通じて復号化ユニット114aへ送る。

【0127】次に、ステップS17で、復号化ユニット114aでは、復号化回路112において、CPU BUS110を通じて受け取った $ES_K'(ES_K(S_K))$ を、第2のセッションキー $S_K'$ を用いて復号し、 $DS_K'(ES_K'(ES_K(S_K)))=ES_K(S_K)$ を得る。

【0128】同様に、ステップS18で、復号化ユニット114aでは、復号化回路112において、CPU BUS110を通じて受け取った $ES_K'(EM_{ki}(S_K))$ を、第2のセッションキー $S_K'$ を用いて復号し、 $DS_K'(ES_K'(EM_{ki}(S_K)))=EM_{ki}(S_K)$ を得る。

【0129】ここで、 $EM_{ki}(S_K)$ を生成する際に用いられたマスターキー $M_{ki}$ は未知であるため、ステップS19において、以下に示すように鍵判定回路120を用いて第1のセッションキー $S_K$ を求める。

【0130】最初に、鍵判定処理の原理について説明する。

【0131】まず、 $EM_{ki}(S_K)$ を、すべてのマスタ



キー $M_{kj}$  ( $j=1\sim n$ ) で夫々復号すると、  
 $S_{kij} = D_{M_{kj}} (E_{M_{ki}} (S_K))$  ( $j=1\sim n$ )  
 が得られる。ここで、 $S_{kij}$  ( $j=1\sim n$ ) のうちのい  
 ずれかが第1のセッションキー $S_K$  である。

【0132】次に、上記の $E_{S_K} (S_K)$  を用いて、生成  
 された $S_{kij}$  ( $j=1\sim n$ ) のいずれが第1のセッシ  
 ョンキー $S_K$  であるかを調べる。

【0133】そこで、 $E_{S_K} (S_K)$  を、すべての第1の  
 セッションキーの候補 $S_{kij}$  ( $j=1\sim n$ ) で夫々復号  
 すると、

$S_k'' (i, j) = D_{S_{kij}} (E_{S_K} (S_K))$   
 が得られる。

【0134】ここで、 $E_{M_{ki}} (S_K)$  を生成する際に用

```
for (i=1; i<n+1; i++) {
    DS1[i] = DMK[i] (EMki (Sk));
    DS2[i] = DSK[i] (ESk (Sk));
    if (DS1[i] == DS2[i])
    {
        SK1=DS2[i];
        break;
    }
    else
}
```

なお、上記手順の2行目は、 $M_{ki}$ を用いて $E_{M_{ki}} (S_K)$  を復号し、これを $DS1[i]$  に代入する  
 操作を示す。

【0137】上記手順の3行目は、 $S_{ki}$ を用いて $E_{S_{ki}} (S_K)$  を復号し、これを $DS2[i]$  に代入する操  
 作を示す。

【0138】上記手順の4行目は、 $DS1[i]$  と $DS2[i]$  が一致するかどうかを判断する操作を示す。

【0139】上記手順の9行目は、 $DS1[i]$  と $DS2[i]$  が不一致の場合の操作を示す。

【0140】さて、例えば図6の鍵判定回路120で  
 は、復号化回路112により、まず、 $j=1$ として、 $E_{M_{ki}} (S_K)$  を、マスターキー $M_{kj}$ で復号して、  
 $S_{kij} = D_{M_{kj}} (E_{M_{ki}} (S_K))$   
 を得る。

【0141】次に、復号化回路112により、 $E_{S_K} (S_K)$  を $S_{kij}$  で復号して、  
 $S_k'' = D_{S_{kij}} (E_{S_K} (S_K))$   
 を得る。

【0142】次に、比較回路121により、上記の  
 $S_k''$  と $S_{kij}$  を比較し、一致した場合、ゲート回路  
 122を制御して、保持しておいた $S_{kij}$  (図6  
 (a)) または $S_k''$  (図6 (b)) を、第1のセッシ  
 ョンキー $S_K$  として出力する。

【0143】一致しなかった場合、上記の $j$  を1ずつ増  
 加させながら、同様の動作を、第1のセッションキー $S_K$  が得られるまで繰り返す。

いられたマスターキー $M_{ki}$ と同一のマスターキー $M_{kj}$ を  
 復号化ユニット内で用いた場合に、すなわち、 $i=j$  の  
 場合に、 $S_k'' (i, j) = S_{kij} = S_K$  となる。

【0135】したがって、各 $S_{kij}$  ( $j=1\sim n$ ) につ  
 いて、 $S_k'' (i, j) = S_{kij}$  ( $j=1\sim n$ ) が成立  
 するか否かを調べることにより、 $S_k'' (i, j) = S_{kij}$  ( $j=1\sim n$ ) を満足する $S_{kij}$  を、第1のセッシ  
 ョンキー $S_K$  として得ることができる。なお、この $S_{kij}$  を与える $j$  に対応するものが今回使用されたマス  
 ターキーである。

【0136】この操作を、C言語の表記を利用してC言  
 語的に表現すると、次のようになる。

```
EXIT_MISMATCH;
```

【0144】以上のようにして第1のセッションキー $S_K$  を得た後、ステップS20で、図示しないDVD駆動  
 装置によりDVD101に記録されている、第1のセッ  
 ションキー $S_K$  を用いて暗号化された画像データ  
 $E_{S_K} (Data)$  を読み出し、暗号ユニット107内に取  
 り込む。その際、復調/誤り訂正回路118により復  
 調、データ中の誤り訂正が行われる。そして、 $E_{S_K} (Data)$  を、CPU BUS110を通じて暗号化ユニ  
 ャット107に送る。

【0145】次に、ステップS21で、復号化ユニット  
 114aでは、復号化回路112において、CPU B  
 US110を通じて受け取った $E_{S_K} (Data)$  を、第  
 1のセッションキー $S_K$  を用いて復号し、  
 $D_{S_K} (E_{S_K} (Data)) = Data$   
 となり、暗号化された画像データを復号して、平文の $Data$  を得ることができる。

【0146】そして、例えば復号すべきデータ (すなわ  
 ち $E_{S_K} (Data)$ ) が終了し、あるいは処理の中止を  
 要求されるまで、上記のステップS20とステップS2  
 1が繰り返し行われる。

【0147】以上のようにして得られた画像データ $Data$  は、例えばMPEG2というデータ圧縮規格に従っ  
 て圧縮されている場合にはMPEGデコーダ回路115  
 でデコードされ、そしてD/A変換回路116でアナロ  
 グ信号に変換された後、図示しないテレビなどの映像装  
 置に送られ、再生される。

【0148】なお、上記のステップS11と、ステップ

S12と、ステップS13およびS14とは、いずれを先に実行しても構わない。

【0149】また、上記のステップS15およびステップS17と、ステップS16およびS18とは、いずれを先に実行しても構わない。

【0150】また、ステップS20とステップS21の実行については、1つの $E_{SK}$  (Data)の単位で逐次行う方法、あるいはステップS20で所定数の $E_{SK}$  (Data)を読み込み、一旦バッファなどへ格納し、次にステップS21でバッファ内の $E_{SK}$  (Data)を復号する方法、あるいはステップS20とステップS21をパイプライン処理的に行う方法などが考えられる。

【0151】また、復号化回路112からMPEGデコーダ回路115に画像データ $E_{SK}$  (Data)を渡す際に、1つのDataの単位で渡しても良いし、所定数のDataの単位で渡しても良い。

【0152】以上のように本実施形態によれば、第1の実施形態と同様に、CPU BUSを流れるデータを保存したとしても、それを再生または利用することはできない。

【0153】この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【0154】また、本実施形態によれば、記録媒体に記録した第1のセッションキーを暗号化するのに用いたマスターキーを直接示す情報が不要であり、DVDなどへの記録の際に予め定められた範囲内で適宜マスターキーを選択して使用することが可能となる。あるいは、DVDの制作・販売会社などの所定の単位ごとに使用可能なマスターキーを割り当てることができるなどの利点がある。

【0155】もちろん、本実施形態でも、暗号化および復号化に用いる回路は、DVDなどのデジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、たとえ暗号が破られたとしても、復号化ユニット114a (あるいは暗号化ユニット107および復号化ユニット114a)を交換するだけで良い。

【0156】なお、本実施形態では、暗号化ユニット107は1つの暗号化回路を持つものとしたが、2つの暗号化回路を設けても良い。また、復号化ユニット114aは1つの復号化回路を持つものとしたが、2、3、4、または5つの復号化回路を設けても良い。これらの場合、対応する暗号化回路と復号化回路をセットで独立化するのが好ましい。

【0157】また、対応する暗号化回路と復号化回路をセットで独立化する場合、独立化した対応する暗号化回路と復号化回路では、他の暗号化回路および復号化回路とは異なる暗号方式を採用しても構わない。

【0158】次に、前述した(方法2)のように、DVD101には $i=1\sim n$ のすべてに対応する $n$ 個の $E$

$M_{ki}$  ( $S_K$ )を記録し、復号化ユニット114a内には $j$ を $1\sim n$ のいずれかとする1つの $M_{kj}$ を備える場合について図7および図8のフローチャートを参照しながら本実施形態の動作を説明する。

【0159】ステップS11で、図示しないDVD駆動装置によりDVD101に記録されている、第1のセッションキー $S_K$ 自身で暗号化された第1のセッションキー $E_{SK}$  ( $S_K$ )を読み出し、暗号ユニット107内に取り込む。その際、復調/誤り訂正回路117により復調、データ中の誤り訂正が行われる。

【0160】また、ステップS12で、図示しないDVD駆動装置によりDVD101に記録されている、マスターキー $M_{ki}$ を用いて暗号化された $n$ 個の第1のセッションキー $E_{M_{ki}}$  ( $S_K$ ) ( $i=1\sim n$ )を読み出し、暗号ユニット107内に取り込む。その際、復調/誤り訂正回路117により復調、データ中の誤り訂正が行われる。

【0161】一方、ステップS13で、復号化ユニット114aでは、セッションキー生成回路111において、乱数、例えば時計(図示せず)からの時間情報を入力として第2のセッションキー $S_K'$ を生成する。そして、復号化回路112において、生成された第2のセッションキー $S_K'$ を、マスターキー $M_{kj}$  (ここで $j$ は $1\sim n$ のうち予め定められたもの)を用いて復号して $D_{M_{kj}}$  ( $S_K'$ )を生成し、CPU BUS110を通じて暗号化ユニット107に送る。

【0162】上記の乱数を発生するタイミング(例えば時間情報を入力するタイミング)としては、例えば、DVD駆動装置にDVD101が装着されたことを示す信号がアサートされたタイミングを用いることができる。

【0163】ステップS14で、暗号ユニット107では、暗号化回路104において、CPU BUS110を通じて受け取った $D_{M_{kj}}$  ( $S_K'$ )を、マスターキーをマスターキー $M_{kj}$  (ここで $j$ は $1\sim n$ のうち予め定められたもの)を用いて暗号化する。すなわち、 $E_{M_{kj}}$  ( $D_{M_{kj}}$  ( $S_K'$ ))) =  $S_K'$ により、復号化ユニット114a内のセッションキー生成回路111で生成された第2のセッションキー $S_K'$ を得ることができる。

【0164】ここで、セッションキー生成回路111で生成された第2のセッションキー $S_K'$ は、CPU BUS110上で盗まれたとしても解らないようにしてある。

【0165】次に、ステップS15で、暗号ユニット107では、上記のようにして得られた第2のセッションキー $S_K'$ を用いて、DVD101に記録された暗号化された第1のセッションキー $E_{SK}$  ( $S_K$ )を暗号化して、 $E_{SK'}$  ( $E_{SK}$  ( $S_K$ )))を生成し、これをCPU BUS110を通じて復号化ユニット114aへ送る。

【0166】同様に、ステップS16で、暗号ユニット

107では、上記のようにして得られた第2のセッションキー $S_K$ を用いて、DVD101に記録された暗号化された $n$ 個の第1のセッションキー $E_{Mki}(S_K)$ を夫々暗号化して、 $E_{SK'}(E_{Mki}(S_K))$ を生成し、これをCPU BUS110を通じて復号化ユニット114aへ送る。

【0167】次に、ステップS17で、復号化ユニット114aでは、復号化回路112において、CPU BUS110を通じて受け取った $E_{SK'}(E_{SK}(S_K))$ を、第2のセッションキー $S_K$ を用いて復号し、 $D_{SK'}(E_{SK'}(E_{SK}(S_K))) = E_{SK}(S_K)$ を得る。

【0168】同様に、ステップS18で、復号化ユニット114aでは、復号化回路112において、CPU BUS110を通じて受け取った $n$ 個の $E_{SK'}(E_{Mki}(S_K))$ を、第2のセッションキー $S_K$ を用いて夫々復号し、 $D_{SK'}(E_{SK'}(E_{Mki}(S_K))) = E_{Mki}(S_K)$ を得る。

【0169】ここで、DVD101に記録されている $n$ 個の $E_{Mki}(S_K)$  ( $i=1\sim n$ )の各々について、それを生成する際に用いられたマスターキー $M_{ki}$ は未知であり、復号化ユニット114a内に備えられたマスターキー $M_{kj}$ に対応するものがどれなのかは、分からないようになっている。そこで、ステップS19において、以下に示すように鍵判定回路120を用いて第1のセッションキー $S_K$ を求める。

【0170】最初に、鍵判定処理の原理について説明する。

【0171】まず、マスターキー $M_{kj}$ で、すべての $E_{Mki}(S_K)$  ( $i=1\sim n$ )を夫々復号すると、 $S_{kij} = D_{Mkj}(E_{Mki}(S_K))$  ( $i=1\sim n$ )が得られる。ここで、 $S_{kij}$  ( $i=1\sim n$ )のうちのいずれかが第1のセッションキー $S_K$ である。

【0172】次に、上記の $E_{SK}(S_K)$ を用いて、生成された $S_{kij}$  ( $i=1\sim n$ )のいずれかが第1のセッションキー $S_K$ であるかを調べる。

【0173】そこで、 $E_{SK}(S_K)$ を、すべての第1のセッションキーの候補 $S_{kij}$  ( $i=1\sim n$ )で夫々復号すると、 $S_{k''}(i, j) = D_{S_{kij}}(E_{SK}(S_K))$ が得られる。

【0174】ここで、 $E_{Mki}(S_K)$ を生成する際に用いられたマスターキー $M_{ki}$ と同一のマスターキー $M_{kj}$ を復号化ユニット内で用いた場合に、すなわち、 $i=j$ の場合に、 $S_{k''}(i, j) = S_{kij} = S_K$ となる。

【0175】したがって、各 $S_{kij}$  ( $i=1\sim n$ )について、 $S_{k''}(i, j) = S_{kij}$  ( $j=1\sim n$ )が成立するか否かを調べることで、 $S_{k''}(i, j) = S_{kij}$  ( $j=1\sim n$ )を満足する $S_{kij}$ を、第1のセッ

ションキー $S_K$ として得ることができる。なお、この $S_{kij}$ を与える $i$ に対応するものが今回使用されたマスターキーである。

【0176】さて、例えば図6の鍵判定回路120では、復号化回路112により、まず、 $i=1$ として、 $E_{Mki}(S_K)$ を、マスターキー $M_{kj}$ で復号して、 $S_{kij} = D_{Mkj}(E_{Mki}(S_K))$ を得る。

【0177】次に、復号化回路112により、 $E_{SK}(S_K)$ を $S_{kij}$ で復号して、 $S_{k''} = D_{S_{kij}}(E_{SK}(S_K))$ を得る。

【0178】次に、比較回路121により、上記の $S_{k''}$ と $S_{kij}$ を比較し、一致した場合、ゲート回路122を制御して、保持しておいた $S_{kij}$  (図6(a))または $S_{k''}$  (図6(b))を、第1のセッションキー $S_K$ として出力する。

【0179】一致しなかった場合、上記の $i$ を1ずつ増加させながら、同様の動作を、第1のセッションキー $S_K$ が得られるまで繰り返す。

【0180】以上のようにして第1のセッションキー $S_K$ を得た後、前述したようにステップS20～S22で、第1のセッションキー $S_K$ を使って、暗号化された画像データ $E_{SK}(\text{Data})$ から画像データ $\text{Data}$ を取り出す。

【0181】そして、前述したように、画像データ $\text{Data}$ は、MPEGデコーダ回路115でデコードされ、D/A変換回路116でアナログ信号に変換されるなどして、図示しないテレビなどの映像装置に送られ、再生される。

【0182】なお、この方法2の場合においても、上記のステップS11と、ステップS12と、ステップS13およびS14とは、いずれを先に実行しても構わない。

【0183】また、上記のステップS15およびステップS17と、ステップS16およびS18とは、いずれを先に実行しても構わない。

【0184】さらに、ステップS12、S16、S18、S19を、DVDに記録された $n$ 個の(暗号化された)マスターキーを一括してバッチ的に行っても良いが、所定数個のマスターキーごとにバッチ的に行っても良いし、1つのマスターキーごとに逐次行っても良い。

【0185】また、3番目の1つのマスターキーごとに逐次行う場合、第2のセッションキー $S_K$ を、マスターキーごとに生成しても良い。

【0186】また、ステップS20とステップS21の実行については、1つの $E_{SK}(\text{Data})$ の単位で逐次行う方法、あるいはステップS20で所定数の $E_{SK}(\text{Data})$ を読み込み、一旦バッファなどへ格納し、次にステップS21でバッファ内の $E_{SK}(\text{Data})$ を復号

する方法、あるいはステップS20とステップS21をパイプライン処理的に行う方法などが考えられる。

【0187】また、復号化ユニット114からMPEGデコーダ回路115に画像データ $E_{SK}$  (Data)を渡す際に、1つのDataの単位で渡しても良いし、所定数のDataの単位で渡しても良い。

【0188】以上のように本実施形態によれば、第1の実施形態と同様に、CPU BUSを流れるデータを保存したとしても、それを再生または利用することはできない。

【0189】この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【0190】また、本実施形態によれば、記録媒体に複数のマスターキーを夫々用いて暗号化した第1のセッションキーと、第1のセッションキー自身で暗号化した第1のセッションキーとを格納するので、復号化ユニット内に作り込むマスターキーを、所定の単位、例えばユニットの製造メーカーごとに割り当てて使用することができるなどの利点がある。

【0191】また、本実施形態でも、暗号化および復号化に用いる回路は、図1から解るようにDVDなどのデジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、たとえ暗号が破られたとしても、復号化ユニット114b (あるいは暗号化ユニット107および復号化ユニット114b)を交換するだけで良い。

【0192】なお、本実施形態では、暗号ユニット107は1つの暗号化回路を持つものとしたが、2つの暗号化回路を設けても良い。また、復号化ユニット114aは1つの復号化回路を持つものとしたが、2、3、4、または5つの復号化回路として設けても良い。これらの場合、対応する暗号化回路と復号化回路をセットで独立化しあるいは共用するのが好ましい。

【0193】また、対応する暗号化回路と復号化回路をセットで独立化する場合、独立化した対応する暗号化回路と復号化回路では、他の暗号化回路および復号化回路とは異なる暗号方式を採用しても構わない。

【0194】次に、前述した(方法3)のように、DVD101には $i=1\sim n$ のすべてに対応する $n$ 個の $E_{MKi}$  ( $S_K$ )を記録し、復号化ユニット114a内には $j$ を $1\sim n$ のうちの $m$  ( $< n$ )種類のものとする $m$ 個の $M_{Kj}$ を備える場合について説明する。

【0195】この方法3は、基本的な構成・動作・効果は上記の方法2と同様であるので、ここでは、相違点のみを説明する。

【0196】上記の方法2では、復号ユニット114a内に予め定めた1個のマスターキー $M_{Kj}$  ( $j=1\sim n$ のいずれか1つ)を備えたが、この方法3では、復号ユニット114a内に予め定めた $m$  ( $\geq 2$ )個のマスターキ

ー $M_{Kj}$ を備えておく。そして、 $m$ 個のマスターキー $M_{Kj}$  ( $j=1\sim n$ のいずれか $m$ 個)について、復号化ユニット114b内で前述した鍵判定に使用する順位を決めておく。

【0197】最初は、DVD101には $i=1\sim n$ のすべてに対応する $n$ 個の $E_{MKi}$  ( $S_K$ )を記録しているので、復号化ユニット114b内で使用順位が1位のマスターキーを用いれば、第1のセッションキー $S_K$ を得ることができるので、この場合には、前述の方法2と同様の動作になる。

【0198】次に、方法3では、いずれかのマスターキーが破られるなどした場合、そのマスターキーを使用不可とし、以降、DVD101には使用不可となったマスターキーに対応する $E_{MKi}$  ( $S_K$ )を記録しないようにした場合を考える。

【0199】ここで、使用不可となったマスターキーが、使用順位が1位のマスターキーでない場合、第1のセッションキー $S_K$ を得ることができるので、この場合にも、前述の方法2と同様の動作になる。

【0200】一方、使用順位が1位のマスターキーが使用不可となった場合、DVD101に該マスターキーに対応する $E_{MKi}$  ( $S_K$ )は記録されていないので、この使用順位が1位のマスターキーを使っても、前述のステップS19にて第1のセッションキー $S_K$ を得ることはできない。このような場合に、復号ユニット114a内で、使用順位が2位のマスターキーを用いて方法2と同様の動作を行うことにより、このマスターキーが使用不可となっていない場合、第1のセッションキー $S_K$ を得ることができる。

【0201】以下、使用順位が $r$ 位のマスターキーが使用不可となっても、使用順位が $r+1$ 位以降のマスターキーで使用不可となっていないものがある場合、同様に第1のセッションキー $S_K$ を得ることができる。

【0202】このようにして、復号化ユニット114a内に予め定めた $m$  ( $\geq 2$ )個のマスターキーが全て使用不可となるまで、本復号化ユニット114aを使用することができる。

【0203】なお、前述した(方法5)の動作は、上記(方法3)と同様になる。

【0204】また、前述した(方法4)は、DVD101には全てのマスターキーに対応する情報が格納されていないので、復号化ユニット内で選択したマスターキーに対応する情報がDVD101に記録されていない場合には、上記の使用不可の場合と同様に復号できないことになり、次の使用順位のマスターキーを選択して復号を試行することになる。従って、この(方法4)の動作も、上記(方法3)と同様になる。

【0205】ところで、本実施形態において、CPU BUS110上を情報を暗号化して安全に転送するために、第2のセッションキー $S_{K'}$ を用いた。この第2の

セッションキー $S_K$ は、復号化ユニット114a内で生成され、マスターキーを用いた手順により暗号化ユニット107に伝えられた。その際、本実施形態では、暗号化ユニット107内には、予め定められた1つのマスターキーが登録されているものとした。

【0206】その代わりに、暗号化ユニット107内にも複数のマスター鍵を登録しておき、鍵判定を用いる前述した(方法1)～(方法5)のような手順を用いて、第2のセッションキー $S_K$ を復号化ユニット114aから暗号化ユニット107に伝えるようにしてもよい。

【0207】例えば、復号化ユニット114a内に登録されているマスターキーと同一のものを暗号化ユニット107にも登録する場合、上記の(方法5)になる。

【0208】また、復号化ユニット114a内に登録されているマスターキーの一部の複数のものを暗号化ユニット107に登録する場合、上記の(方法3)になる。

【0209】なお、暗号化ユニット107に1つのマスターキーを登録する場合にも、上記の(方法2)の手順を用いることができる。

【0210】ただし、これらの場合、(方法1)～(方法5)の手順において、暗号化と復号とを入れ替えた手順となる。すなわち、復号化ユニット114aから暗号化ユニット107に $D_{Mki}(S_K)$ と $D_{SK}(S_K)$ とを転送することになる。

【0211】なお、第2のセッションキー $S_K$ をCPU BUS110上を介して復号化ユニット114aから暗号化ユニット107に安全に伝えるための構成としては、上記のマスターキーを用いる構成の他にも、種々のものが適用可能である。例えば、「日経エレクトロニクス No. 676 pp. 13-14 1996. 1. 18」に開示された技術を応用することもできる。この場合、暗号化ユニット107内へのマスターキーの登録は不要である。

【0212】(第3の実施形態)次に、第3の実施形態について説明する。

【0213】本実施形態は、例えば単体のDVDプレーヤーである。

【0214】図9は、本発明の第2の実施形態に係るシステムの構成を示すブロック図である。また、本実施形態の動作の一例を図10のフローチャートに示す。

【0215】本実施形態は、第2の実施形態の構成から、暗号化ユニットと復号ユニットとの間で第2のセッションキーを用いて暗号化鍵を受け渡しする動作に関する部分を削除したものである。

【0216】すなわち、図9に示すように、本実施形態に係るシステムは、DVD101からデータの読み出すDVD駆動装置(図示せず)、復号化ユニット114bを備えている。

【0217】復号化ユニット114bは、復号化回路112、鍵判定回路120、復調/誤り訂正回路117、

復調/誤り訂正回路118を備えている。また、本実施形態では、復号化ユニット114内にMPEGのデコーダ回路115および復号された画像データをデジタルからアナログに変換する変換回路116を備えているものとする。

【0218】ここで、鍵判定回路120は、図6の一構成例に示すように、復号化回路112、比較回路121、ゲート回路122を備えている。

【0219】図9および図6中で、復号化ユニット114b内には、鍵判定回路120内の2つの復号化回路112を含めて、全部で3つの復号化回路112を示しているが、実際には1つの復号化回路であるものとする。なお、復調/誤り訂正回路117および復調/誤り訂正回路118は、暗号化ユニット107内には備えず、その前段のユニット等の側に備えられる場合もある。

【0220】復号化ユニット114bは、独立した1つのICチップとして形成されるものとする。

【0221】また、復号化ユニット114b内には、後述するマスターキーが登録されている(作り込まれている)。マスターキーは、利用者が外部から取得できないように、復号化ユニットのチップにおいて、利用者が意図的に取り出せないようにチップ内部の秘匿された領域に記録されているものとする。

【0222】本実施形態では、第1のセッションキーを $S_K$ 、第2のセッションキーを $S_K$ 、 $n$ 種類存在するマスターキーのうちの $i$ 番目のものを $M_{ki}$ (ここで $i=1\sim n$ )、画像データ(ただし、暗号化された一纏まりのデータ)を $Data$ で表す。これらはいずれも平文である。

【0223】図1中、102-1は第1のセッションキー $S_K$ をマスターキー $M_{ki}$ を用いて暗号化して生成された $E_{Mki}(S_K)$ を、102-2は第1のセッションキー $S_K$ を第1のセッションキー $S_K$ 自身で暗号化して生成された $E_{SK}(S_K)$ を、103は画像データ $Data$ を第1のセッションキー $S_K$ を用いて暗号化して生成された $E_{SK}(Data)$ を、105はマスターキー $M_{kj}$ を、113は第1のセッションキー $S_K$ をそれぞれ表す。

【0224】ここで、前述の第2の実施形態と同様に、DVD101に記録する第1のセッションキー $S_K$ をマスターキー $M_{ki}$ を用いて暗号化して生成された $E_{Mki}(S_K)$ の種類数と、復号化ユニット114b内に持つマスターキー $M_{kj}$ の種類数の設定について、例えば次に示すように幾つかの方法が考えられる。

【0225】(方法1) DVD101には $i=1\sim n$ のいずれかとする1つの $E_{Mki}(S_K)$ を記録し、復号化ユニット114b内には $j=1\sim n$ のすべてに対応する $n$ 個の $M_{kj}$ を備える。

【0226】(方法2) DVD101には $i=1\sim n$ のすべてに対応する $n$ 個の $E_{Mki}(S_K)$ を記録し、復号

化ユニット114b内にはjを1～nのいずれかとする1つのM<sub>kj</sub>を備える。

【0227】(方法3) DVD101にはi=1～nのすべてに対応するn個のE<sub>Mki</sub>(S<sub>k</sub>)を記録し、復号化ユニット114b内にはjを1～nのうちのm(2<m<n)種類のものとするm個のM<sub>kj</sub>を備える。

【0228】(方法4) DVD101にはiを1～nのうちのから予め選択されたm(2<m<n)種類のものとするm個のマスターキーE<sub>Mki</sub>(S<sub>k</sub>)を記録し、復号化ユニット114b内にはj=1～nのすべてに対応するn個のマスターキーM<sub>kj</sub>を備える。

【0229】(方法5) DVD101にはi=1～nのすべてに対応するn個のマスターキーE<sub>Mki</sub>(S<sub>k</sub>)を記録し、復号化ユニット114b内にはj=1～nのすべてに対応するn個のマスターキーM<sub>kj</sub>を備える。

【0230】図3に示すように、DVD101上で、第1のセッションキーS<sub>k</sub>をマスターキーM<sub>ki</sub>を用いて暗号化して生成された1個(上記の(方法1)の場合)または複数個(上記の(方法2)～(方法5)の場合)のE<sub>Mki</sub>(S<sub>k</sub>)は、最内周部分の鍵記録領域(リードインエリア)に、画像データDataを第1のセッションキーS<sub>k</sub>を用いて暗号化して生成されたE<sub>Sk</sub>(Data)は、データ記録領域(データエリア)に記録されているものとする。

【0231】次に、図10のフローチャートを参照しながら本実施形態の動作について説明する。なお、本実施形態の動作は、第2の実施形態の動作から、暗号化ユニットと復号ユニットとの間で第2のセッションキーを用いて暗号化鍵を受け渡しする動作に関する部分を削除したものである。

【0232】すなわち、ステップS31で、図示しないDVD駆動装置によりDVD101に記録されている、第1のセッションキーS<sub>k</sub>自身で暗号化された第1のセッションキーE<sub>Sk</sub>(S<sub>k</sub>)を読み出し、復号化ユニット114b内に取り込む。その際、復調/誤り訂正回路117により復調、データ中の誤り訂正が行われる。

【0233】また、ステップS32で、図示しないDVD駆動装置によりDVD101に記録されている、マスターキーM<sub>ki</sub>を用いて暗号化された第1のセッションキーE<sub>Mki</sub>(S<sub>k</sub>)を読み出し、復号化ユニット114b内に取り込む。その際、復調/誤り訂正回路117により復調、データ中の誤り訂正が行われる。

【0234】次に、ステップS33において、鍵判定回路120を用いて第1のセッションキーS<sub>k</sub>を求める。

【0235】以上の第1のセッションキーS<sub>k</sub>を求める動作は、(方法1)、(方法2)、(方法3～方法5)により相違するが、いずれの場合についても既に第2の実施形態において説明したものと同様であるので、ここでの説明は省略する。

【0236】第1のセッションキーS<sub>k</sub>を得た後は、前

述したようにステップS34～S36で、第1のセッションキーS<sub>k</sub>を使って、暗号化された画像データE<sub>Sk</sub>(Data)から画像データDataを取り出す。なお、ステップS34～S36の動作は、ユニット間でCPU BUSを介した画像データDataの受け渡しが無い以外は、第2の実施形態において既に説明したステップS20～S22(すなわち、第1の実施形態において既に説明したステップS6～S8)と同様である。

【0237】そして、前述したように、画像データDataは、MPEGデコーダ回路115でデコードされ、D/A変換回路116でアナログ信号に変換されるなどして、図示しないテレビなどの映像装置に送られ、再生される。

【0238】なお、この方法3の場合においても、上記のステップS31と、ステップS32とは、いずれを先に実行しても構わない。

【0239】また、(方法2)および(方法3～5)の場合において、ステップS32、S33を、DVDに記録されたn個(方法2、3、5の場合)あるいはm個(方法4の場合)の(暗号化された)マスターキーを一括してバッチ的に行っても良いが、所定数個のマスターキーごとにバッチ的に行っても良いし、1つのマスターキーごとに逐次行っても良い。

【0240】また、ステップS34とステップS35の実行については、1つのE<sub>Sk</sub>(Data)の単位で逐次行う方法、あるいはステップS20で所定数のE<sub>Sk</sub>(Data)を読み込み、一旦バッファなどへ格納し、次にステップS21でバッファ内のE<sub>Sk</sub>(Data)を復号する方法、あるいはステップS20とステップS21をパイプライン処理的に行う方法などが考えられる。

【0241】また、復号化ユニット114からMPEGデコーダ回路115に画像データE<sub>Sk</sub>(Data)を渡す際に、1つのDataの単位で渡しても良いし、所定数のDataの単位で渡しても良い。

【0242】本実施形態によれば、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【0243】また、本実施形態によれば、DVDなどへの記録の際に予め定められた範囲内で適宜マスターキーを選択して使用することが可能となる。あるいは、DVDプレーヤーのメーカーまたはDVDの制作・販売会社などの所定の単位ごとに使用可能なマスターキーを割り当てて使用することができるなどの利点がある。

【0244】また、本実施形態では、暗号化および復号化に用いる回路は、図1から解るようにDVDなどのデジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、たとえ暗号が破られたとしても、復号化ユニット114bを交換するだけで良い。

【0245】なお、本実施形態では、復号化ユニット114bは1つの復号化回路を持つものとしたが、2また

は3つの復号化回路として設けても良い。これらの場合、対応する暗号化回路と復号化回路をセットで独立化しあるいは共用するのが好ましい。

【0246】また、対応する暗号化回路と復号化回路をセットで独立化する場合、独立化した対応する暗号化回路および復号化回路では、他の暗号化回路および復号化回路とは異なる暗号方式を採用しても構わない。

【0247】以上、第1の実施形態、第2の実施形態（より詳しくは3種類の構成）、第3の実施形態（より詳しくは3種類の構成）について夫々説明してきたが、本発明はこれらに限定されず種々変形して実施することができる。

【0248】各実施形態では、情報の記録媒体をDVDとして説明したが、本発明は、CD-ROM等他の記録媒体にも適用可能である。

【0249】各実施形態では、復号対象となる情報として画像データを例にとって説明したが、本発明は、音声、テキスト、プログラムなど、他の形態の情報の再生装置等にも適用可能である。

【0250】なお、各実施形態では、データDataを画像データとしたが、データDataを鍵情報Sk<sub>t</sub>とする構成も考えられる。すなわち、DVD等の記録媒体に、ESK(Data)の代わりに、ESK(Sk<sub>t</sub>)とESk<sub>t</sub>(Data)を記録しておき、復号化ユニット114、114a、114bにおいて各実施形態で示した手順により、まずSk<sub>t</sub>を得て、このSk<sub>t</sub>でESk<sub>t</sub>(Data)を復号して実際のコンテンツを得るようにすることもできる。また、このような鍵の階層化は、任意の階層に渡って行うことができる。

【0251】各実施形態では、復号対象となる情報がMPEG2という規格に従って圧縮されている場合を例にとって説明したが、本発明はこれに限定されず、他の規格によってデータ圧縮あるいは符号化等されていても構わない。この場合、MPEGデコーダ回路115の代わりに、他の対応するデコーダ回路を設ける。また、符号化等されていないものであっても構わない。この場合、MPEGデコーダ回路115を削除する。

【0252】また、種々の方式で圧縮等されたデータ（あるいは復号の必要ないデータ）のいずれも出力できるように、複数種類のデコード回路等を設け、これを適宜切替て使用し（あるいはこれらを使用しないように）構成することも可能である。この場合、例えば、DVD等の記録媒体から使用すべきデコード等を示す識別子を読み込む、この識別子に従って適切なデコード回路等を選択する方法が考えられる。

【0253】第2の実施形態および第3の実施形態にて示した図6の鍵判定回路120の構成は一例であり、この他にも種々の構成が考えられる。

【0254】さらに、鍵判定用情報としてESK(S<sub>K</sub>)を用いる構成は、この他にも種々のものが考えられる。

例えば、鍵判定に用いる情報としてDSK(S<sub>K</sub>)を用い、鍵判定回路120では、DVD等の記録媒体から読み込んだEmk<sub>i</sub>(S<sub>K</sub>)を記憶されたマスターキーMk<sub>j</sub>で復号してSk<sub>ij</sub>=Dmk<sub>j</sub>(Emk<sub>i</sub>(S<sub>K</sub>))を得て、このSk<sub>ij</sub>をSk<sub>ij</sub>自身で復号してSk'''=DSk<sub>ij</sub>(Sk<sub>ij</sub>)を得て、次に、このSk'''とDVD等の記録媒体から読み込んだDSK(S<sub>K</sub>)を比較し、一致した場合、第1のセッションキーS<sub>K</sub>=Sk<sub>ij</sub>は正しいものと判定して出力する。

【0255】また、鍵判定用情報の他の例として、2回以上暗号化または復号を行ったもの、例えば、ESK(ESK(S<sub>K</sub>))、DSK(DSK(S<sub>K</sub>))、あるいは各Emk<sub>i</sub>(S<sub>K</sub>)に対応してEmk<sub>i</sub>(Emk<sub>i</sub>(S<sub>K</sub>))を設けるものなど種々のものが考えられる。

【0256】また、各実施形態では、鍵判定用情報をもとに（方法1）～（方法5）で示した手順を用いて、復号により得られた鍵が第1のセッションキーが正しいものであることを判定したが、DVD等の記録媒体にiの順番ですべてのEmk<sub>i</sub>(S<sub>K</sub>)を記録しておき、復号ユニットにはiとMk<sub>i</sub>を対応付けて登録しておくことにより、鍵判定用情報、鍵判定手順、そのための構成を省略することができる。なお、あるiについてのMk<sub>i</sub>が使用不可となった場合には、DVD等の記録媒体にEmk<sub>i</sub>(S<sub>K</sub>)の代わりに無効を示す情報を格納するのが望ましい。

【0257】次に、図11を参照しながら、DVD-ROMを例に取り上げ、上記した第3の実施形態を用いたディスクメーカ（映画、音楽等の著作物のDVDを制作するメーカとする）とプレーヤメーカ（単体のDVDプレーヤのメーカとする）とマスターキーを管理する鍵管理組織による鍵の管理方法等について説明する。なお、Dataは、コンテンツの他に、前述したように鍵情報である場合もある（Dataが鍵情報Sk<sub>t</sub>である場合のこの鍵情報Sk<sub>t</sub>を用いた暗号化や復号等についての説明は省略する）。なお、図11において、処理等に用いる計算機等については省略してある。

【0258】また、図12には暗号化のためのシステムに関して説明するための図を示す。図12の暗号化回路301、312、303は、同一の装置（計算機等）上に搭載される場合と、異なる装置（計算機等）上に搭載される場合があり、後者の場合には、装置間で情報の受け渡しが行われる。また、暗号化回路301、312、303は、ハードウェアで構成することも、ソフトウェアで構成することも可能である。

【0259】ここでは、上記した（方法3）のDVDにはi=1～nのすべてに対応するn個のマスターキーEmk<sub>i</sub>(S<sub>K</sub>)を記録し、DVDプレーヤ（復号化ユニット114b）内にはjを1～nのうちのから予め選択されたm（2<m<n）種類のものとするm個のマスターキーMk<sub>j</sub>を備える場合について説明する。なお、DVD

プレーヤメカにはマスターキー $M_{kj}$ を排他的に割り当てるものとする。また、ここでは、 $n=100$ 、 $m=10$ とする。

【0260】また、ここでは、鍵判定用情報として、DVDには $ESK(S_k)$ を記録する方法を用いるものとする(図12の302の部分は、鍵判定用情報を $ESK(S_k)$ とした場合のものである)。

【0261】まず、鍵管理組織200では、マスターキー $M_{ki}$  ( $i=1\sim100$ )を保管している。マスターキーに数は、プレーヤメカの新規参入や破られた場合の予備等のために、余分に設定しておくのが望ましい。

【0262】鍵管理組織200では、各プレーヤメカ201~203に、排他的にマスターキー $M_{ki}$  ( $i=1\sim100$ )を割り当てる。例えば、図11のように、プレーヤメカAにマスターキー $M_{ki}$  ( $i=10\sim19$ )を、プレーヤメカBにマスターキー $M_{ki}$  ( $i=20\sim29$ )を、プレーヤメカCにマスターキー $M_{ki}$  ( $i=30\sim39$ )を割り当てる。鍵管理組織200(の計算機等)から各プレーヤメカ(の計算機等)には、割り当てたマスターキーを通信媒体あるいは記録媒体等により送付する。その際、暗号通信等を用いて安全に受け渡しするのが望ましい。

【0263】各プレーヤメカは、個別に、鍵管理組織200から割り当てられたマスターキーを管理する。そして、各プレーヤメカは、この割り当てられたマスターキーを用いて、第3の実施形態で示したような構成を有するDVDプレーヤを製造して販売する。

【0264】一方、ここでは、鍵管理組織200からディスクメカ221~223へは、マスターキーのプレインデータは渡さないようにするものとする。

【0265】まず、各ディスクメカ(aとする)は、自身で第1のセッションキー $S_k$ を決め(例えばディスク毎に決め)、第1のセッションキー $S_k$ を鍵管理組織200に渡す。鍵管理組織200は、受け取った第1のセッションキー $S_k$ を全てのマスターキー $M_{ki}$  ( $i=1\sim100$ )でそれぞれ暗号化して $E_{Mki}(S_k)$ 、( $i=1\sim100$ )を得る(図12の暗号化回路301を用いる)。そして、鍵管理組織200は、 $E_{Mki}(S_k)$ 、( $i=1\sim100$ )を、ディスクメカaに渡す。

【0266】鍵管理組織200(の計算機等)とディスクメカ(の計算機等)との間での情報の受け渡しも、上記と同様に、割り当てたマスターキーを通信媒体あるいは記録媒体等にて暗号通信等を用いて安全に行うのが望ましい。

【0267】ディスクメカaでは、 $E_{Mki}(S_k)$ 、( $i=1\sim100$ )と、 $ESK(S_k)$ と、 $ESK(Data)$ とをDVD231に記録して販売する。なお、 $S_k$ 自身で $S_k$ を暗号化して $ESK(S_k)$ を得る操作は、ディスクメカ側で行う方法と、マスターキーによる暗

号化と同様に鍵管理組織200側で行う方法とがある(図12の暗号化回路312を用いる)。また、少なくとも、コンテンツの暗号化はディスクメカにて行うものとする(図12の暗号化回路303を用いる)。

【0268】ディスクメカaでは、例えば、 $S_k$ について、受け取った $E_{Mki}(S_k)$ と鍵判定用情報である $ESK(S_k)$ と $ESK(Data)$ (あるいは $Data$ )について管理する。

【0269】他のディスクメカについても同様である。

【0270】なお、万一、マスターキーが破られたことが発覚した場合、それ以降、その破られたマスターキーを用いずに、DVDを制作するようにする。例えば、 $i=19$ のマスターキーが破られた場合、DVDには、 $i=1\sim18$ 、 $20\sim100$ の99個に対応する $E_{Mki}(S_k)$ が記録される。

【0271】また、マスターキーが破られたことが発覚した場合、それ以降、その破られたマスターキーが割り当てられているプレーヤメカでは、これを除いてDVDプレーヤを製造して販売するようにするのが望ましい。例えば、 $i=19$ のマスターキーが破られた場合、プレーヤメカAは、 $i=10\sim18$ のマスターキーを用いてDVDプレーヤを製造して販売する。

【0272】また、既に販売された $i=19$ のマスターキーを持つてDVDプレーヤについては、そのまま使用しても構わない。ただし、ユニット交換等によって $i=19$ のマスターキーを持たないようにしてもよい。

【0273】従って、マスターキーを安全かつ有効に管理できるとともに、不正なマスターキー解読に対するリスクを分散し、マスターキー解読後も上記システムが安全かつ有効に機能するようにすることができる。

【0274】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0275】

【発明の効果】本発明によれば、複数の第2の鍵のうちの少なくとも1つを持つ正当なもののみが、第1の鍵を得ることができ、従って第1の鍵で暗号化されたデータのプレインデータを得ることができる。

【0276】この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係るシステムの構成を示すブロック図

【図2】同実施形態の動作を示すフローチャート

【図3】記録媒体に暗号化された鍵と暗号化されたデータを格納する形式の一例を示す図

【図4】CPU BUSからデータを保存した場合について説明するための図



【図5】本発明の第2の実施形態に係るシステムの構成を示すブロック図

【図6】鍵判定部の内部構成の例を示す図

【図7】同実施形態の動作を示すフローチャート

【図8】同実施形態の動作を示すフローチャート

【図9】本発明の第3の実施形態に係るシステムの構成を示すブロック図

【図10】同実施形態の動作を示すフローチャート

【図11】鍵の管理方法について説明するための図

【図12】暗号化について説明するための図

【符号の説明】

101…DVD

102, 202…マスターキーを用いて暗号化された第1のセッションキー

103, 203…第1のセッションキーを用いて暗号化された画像データ

104…暗号化回路

105…マスターキー

106…第2のセッションキー

107…暗号化ユニット

108…マスターキーを用いて復号された第2のセッシ

ョンキー

109…第2のセッションキーを用いて暗号化された、マスターキーを用いて暗号化された第1のセッションキー

110…CPU BUS

111…セッションキー生成回路

112…復号化回路

113…第1のセッションキー

114, 114a, 114b…復号化ユニット

115…MPEGデコーダ回路

116…デジタル/アナログ変換回路

209…DVDの読み出し出力から別の媒体にコピーするための線

210…CPU BUSから別の媒体にコピーするための線

211…デジタル記憶媒体

200…鍵管理組織

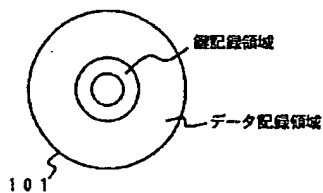
201～203…プレーヤメーカ

221～223…ディスクメーカ

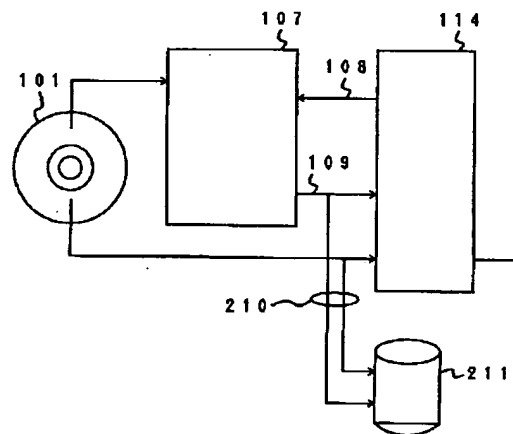
231～233…DVD

301, 312, 303…暗号化回路

【図3】

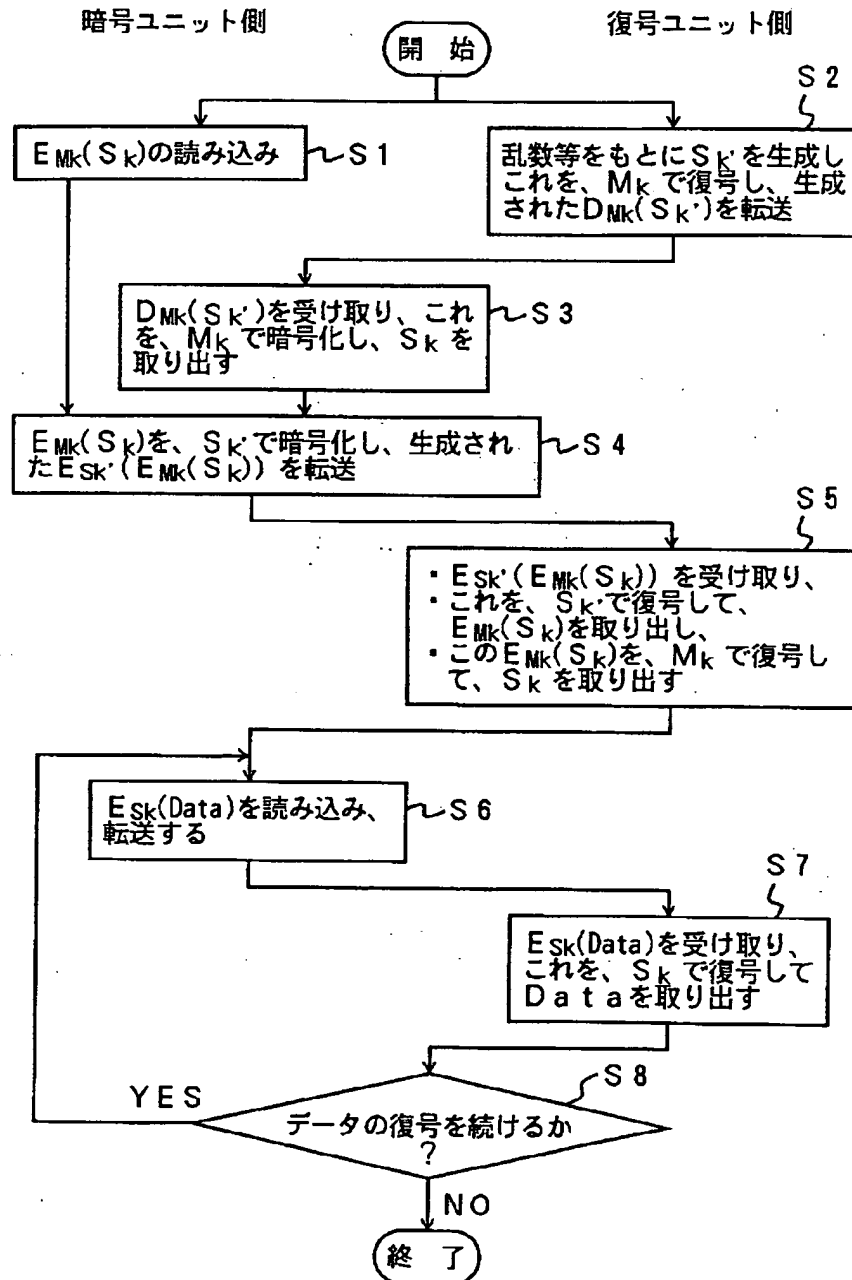


【図4】



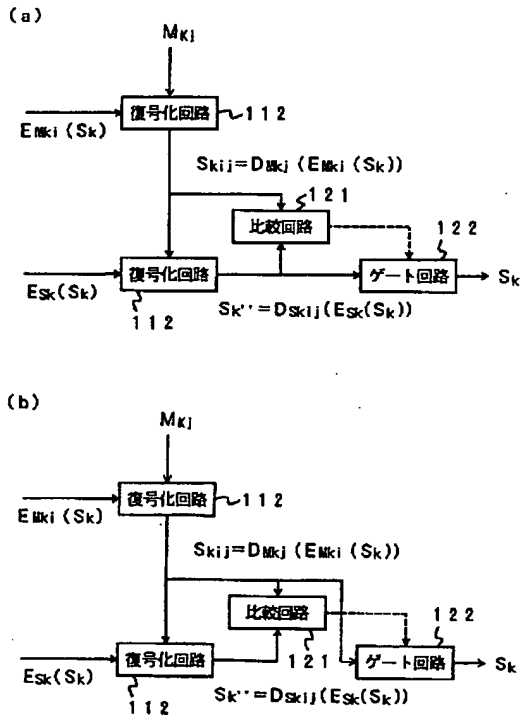


【図2】

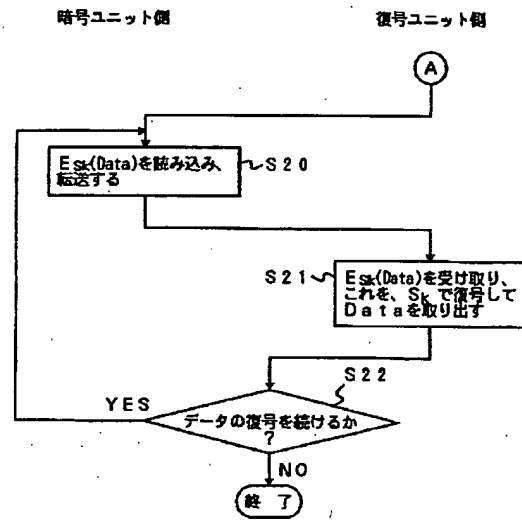




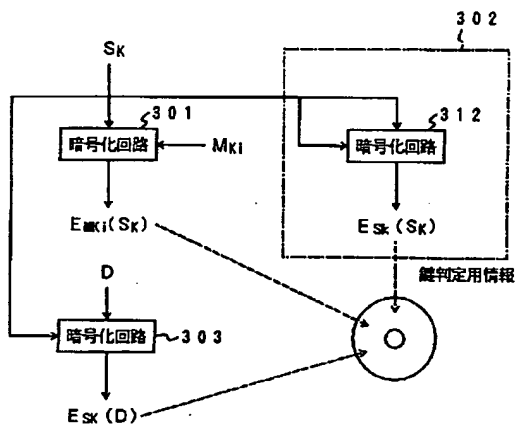
【図6】



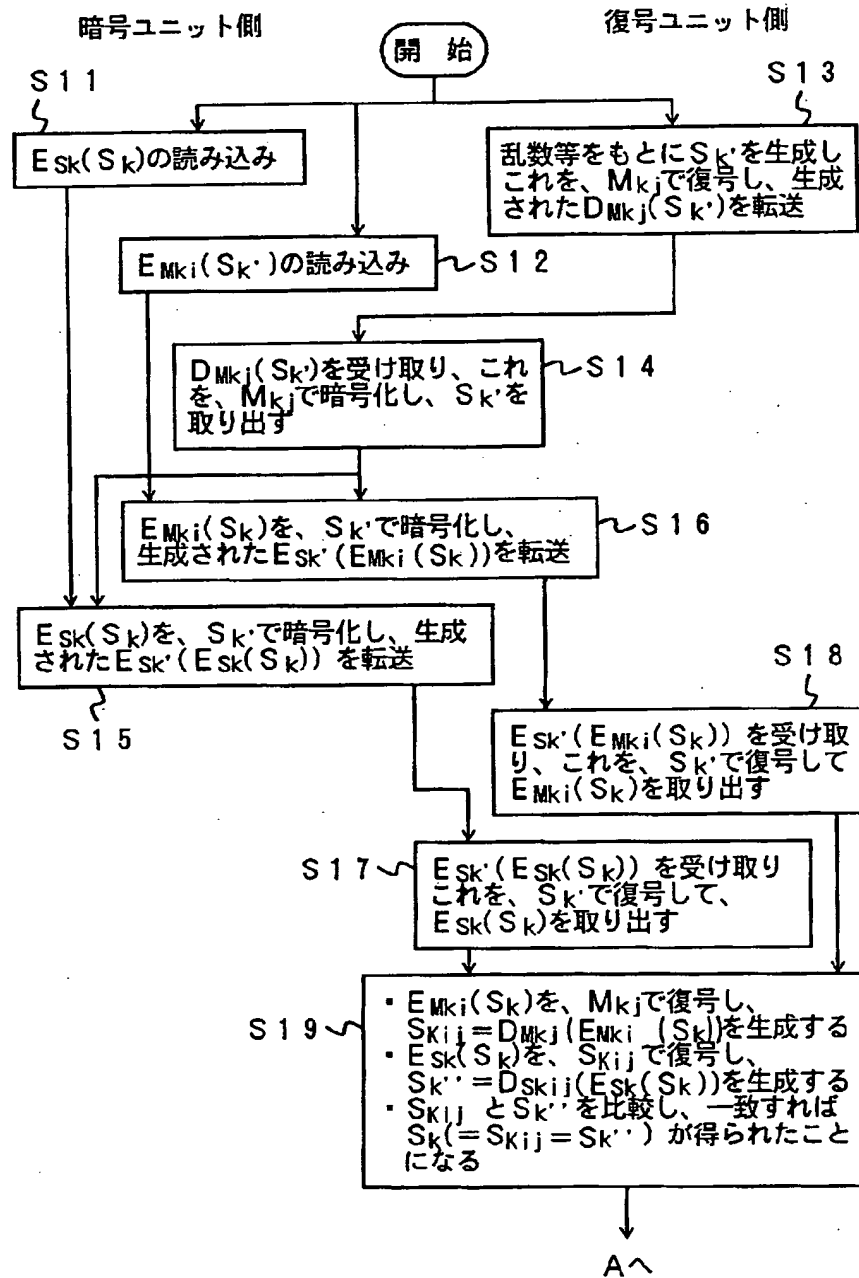
【図8】



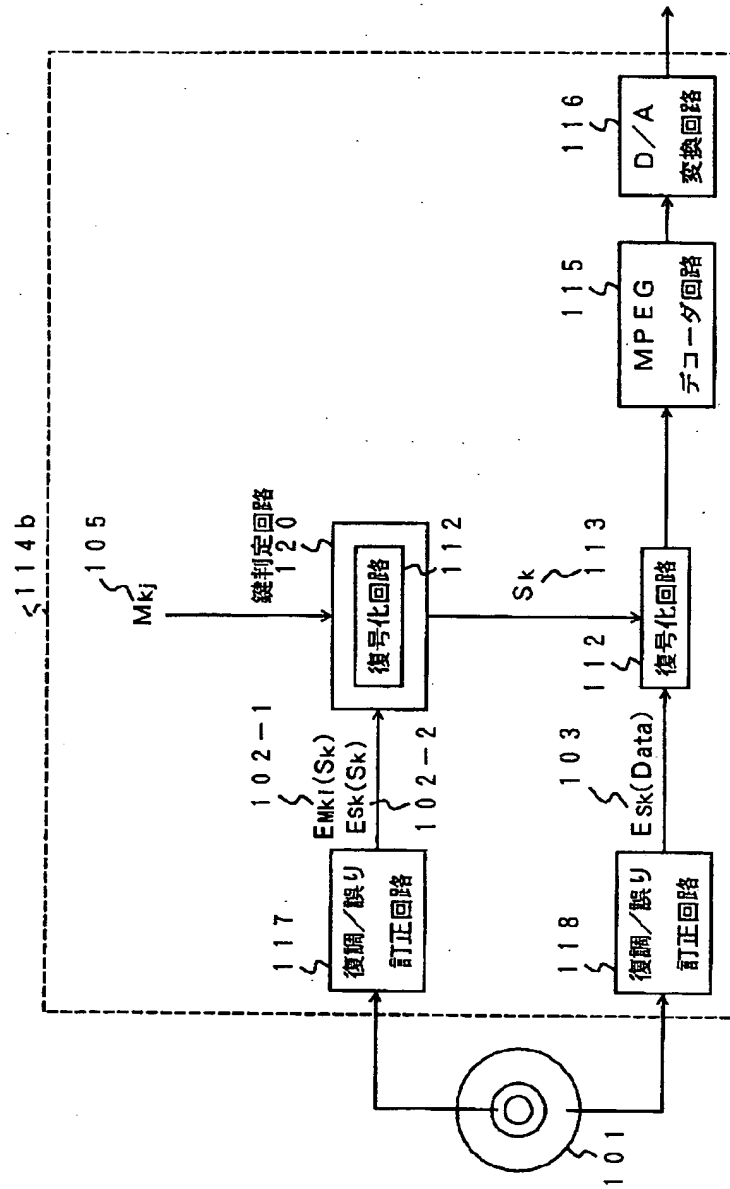
【図12】



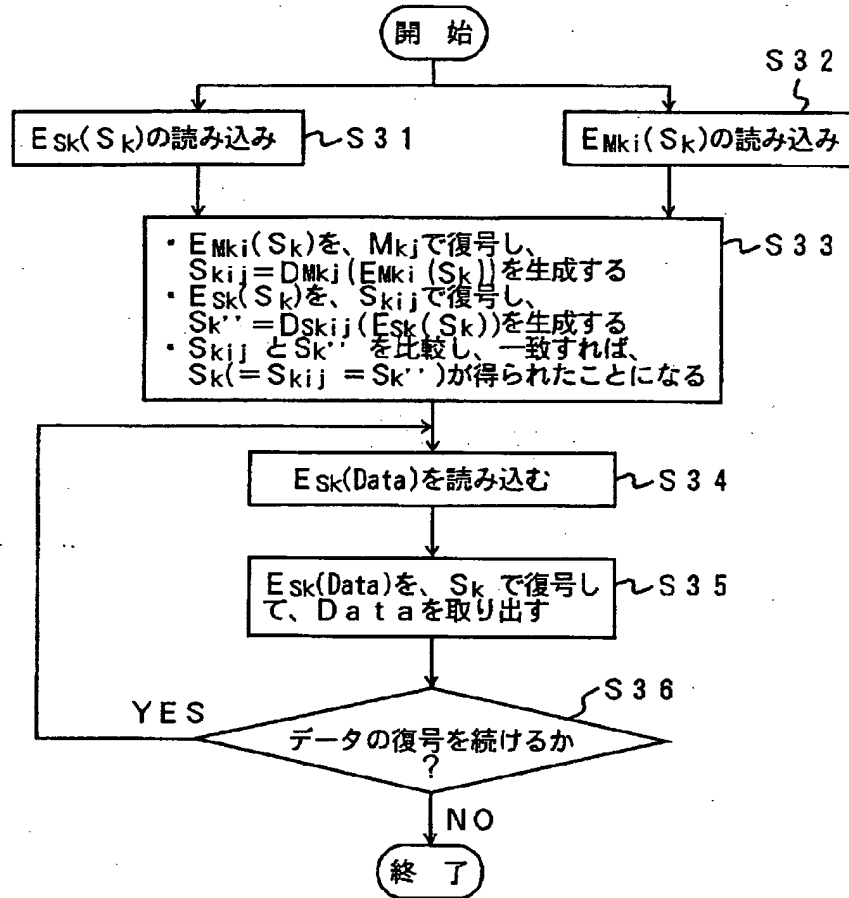
【図7】



【図9】

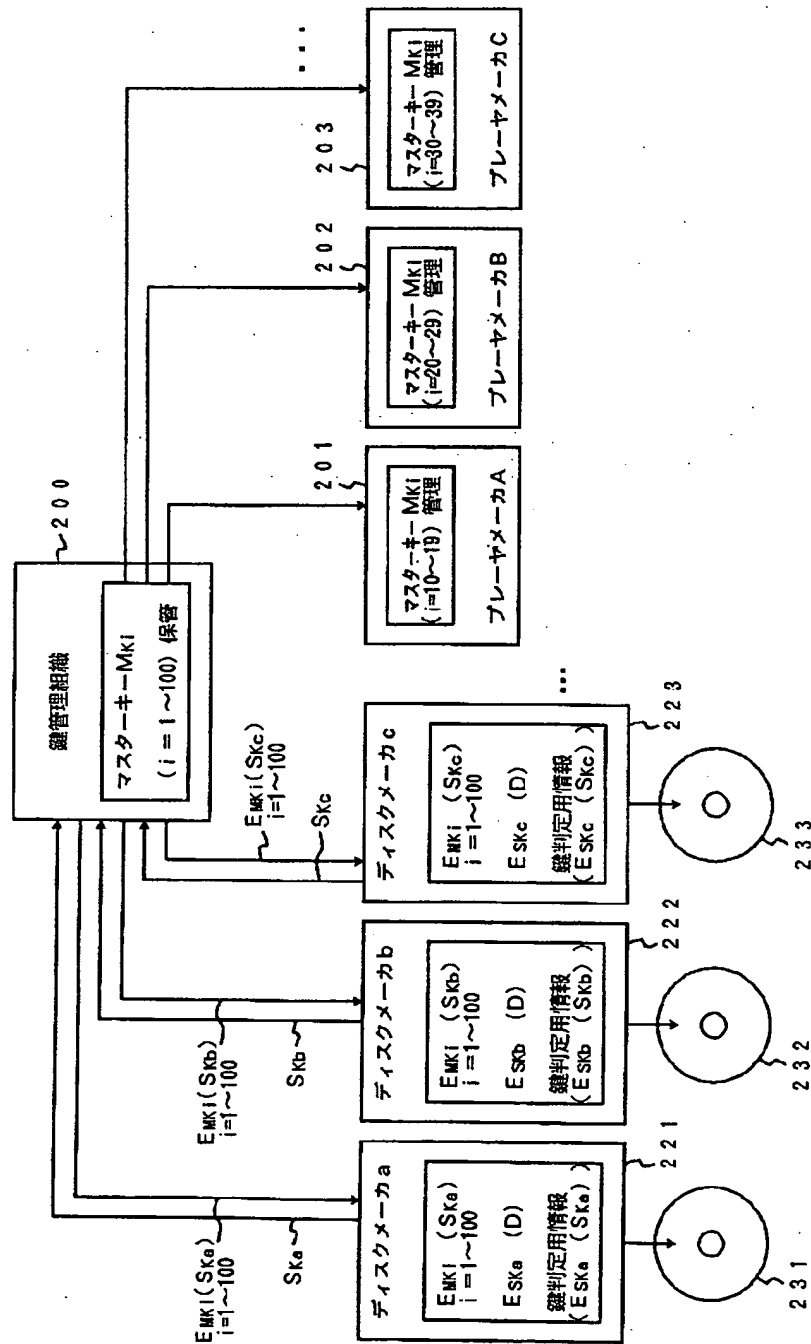


【図10】





【図11】



フロントページの続き

(51) Int. Cl. 6

識別記号

F I  
H 04 L 9/00601 E  
601 B

(72)発明者 小島 正

神奈川県川崎市幸区柳町70番地 株式会社  
東芝柳町工場内

(72)発明者 平山 康一

神奈川県川崎市幸区柳町70番地 株式会社  
東芝柳町工場内